尽 善 尽 美  弗 求 弗 迪

A Brief History of

The Hackers

黑客简史

棱镜中的帝国

刘创 著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

“黑客”，伴随着计算机和互联网而诞生，他们掌握着前沿的计算机和网络技术，能够发现并利用计算机系统和网络的弱点，他们的行为动机多样，因此我们必须对这一群体进行分解，认识他们及其技术的两面性——“黑客”中那些不断拓展技术边界、富于创造力的，和那些掌握技术、却利欲熏心的，就像硬币的两面，谁都无法清晰地辨别是非。相对于主流文化，黑客的行为方式和理念等形成了一种“亚文化”，与主流文化相互作用。

图书在版编目（CIP）数据

黑客简史：棱镜中的帝国 / 刘创著. —北京：电子工业出版社，2015.01
ISBN 978-7-121-24393-6

Ⅰ. ①黑… Ⅱ. ①刘… Ⅲ. ①计算机网络—安全技术—研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2014）第220041号

责任编辑：杨 雯
印 刷：三河市兴达印务有限公司
装 订：三河市兴达印务有限公司
出版发行：电子工业出版社
北京市海淀区万寿路173信箱 邮编：100036
开 本：720×1000 1/16 印张：17.75 字数：264千字
版 次：2015年01月第1版
印 次：2015年01月第1次印刷
定 价：39.80元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

出版者的话：从棱镜门说起

在“棱镜门”让全世界坐立不安之时，我们推出这本《黑客简史：棱镜中的帝国》，透过“黑客”的个案看到本质，在“棱镜门”沸沸扬扬之后进行一种冷思考。

“黑客”，伴随着计算机和互联网而诞生，他们掌握着前沿的计算机和网络技术，能够发现并利用计算机系统和网络的弱点，他们的行为动机多样，因此我们必须对这一群体进行分解，认识他们及其技术的两面性——“黑客”中那些不断拓展技术边界，富于创造力的人，无疑是值得推崇和赞扬的；而那些掌握技术，却利欲熏心、为非作歹之徒，虽然能逞一时之快，但终究难逃恶果。相对于主流文化，黑客的行为方式和理念等形成了一种“亚文化”，与主流文化相互作用。

黑客们的活动范围早已今非昔比，当网络的边界和深度不断扩张之时，人们面对的机遇与风险也在同比例地放大；同时，云计算、大数据等网络发展与应用的新技术，人们的日常生活大多已完全依赖这些技术的应用。

美国“棱镜”项目的设计与实施无不得益于当前的社会化媒体。正是因为网络技术的发展应用以及网络世界的无国界性，使得“棱镜”项目监视的范围涉及全球多个国家和地区，中国无疑也是该项目重点监视的地区之一。据中国国家互联网应急中心的报告显示，仅2012年就有7.3万个境外IP地址参与了控制中国境内1400余万台主机的网络攻击事件；有3.2万个境外IP地址通过植入后门，对中国境内3.8万个网站进行了远程控制。[①]

① 我国信息安全问题的检视与反思．光明日报．2013-08-09

现在全球共有13台根域名服务器，其中有10台设置在美国，另外在英国、瑞典和日本各设置有一台。由此可见，美国对互联网拥有绝对的控制权。因此，技术进步固然重要，而更加重要、更具现实意义，关系到现实利益的，是技术掌握在谁的手中，被用于何处。此次的“棱镜门”事件，让乔治·奥威尔的科幻讽刺小说《1984》中的“老大哥”无处不在、无孔不入的监视能力从幻想走向了现实，“棱镜”计划的监视能力及范围同“老大哥”相比，是有过之而无不及的，其对各个国家政府信息的刺探和个人隐私的侵犯，让世人不寒而栗。

中国政府始终坚决反对任何形式的网络攻击行为，坚持依法管理，不断完善互联网管理方面的法律法规，在《刑法》、《治安管理处罚法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》、《计算机信息系统安全保护条例》、《电信条例》、《计算机病毒防治管理办法》等多项法律法规中，对打击网络攻击等犯罪行为做出了明确规定。2009年，工信部先后出台了《互联网网络安全信息通报实施办法》和《木马和僵尸网络监测和处置机制》，先后多次组织专项治理行动，有效遏制了木马和僵尸网络传播；组织270多家单位共同开展网络安全事件的监测、预警和应急处置，国家互联网应急中心仅2009年就有效处置网络安全事件1100多起，为多家银行、电子商务网站和用户挽回了经济损失。同时，积极开展行业自律工作，指导中国互联网协会组织基础电信运营企业、网络安全厂商、增值服务提供商、搜索引擎、域名注册机构等成立了“中国反网络病毒联盟”并签署自律公约，净化了网络环境，维护公共互联网网络安全[①]。

网络环境是全民共享的，只有整个社会行动起来，每个人都自觉自愿自律，网络安全才能被更好地维护。同时，我们相信，那些处于技术和道德制高点的黑客会一直促进电脑技术和互联网的发展，他们对于技术的追求永远不会停止，并以自己的方式改变着世界。

① 工信部驳斥“中国黑客与黑客攻击”说．新华网．2010-01-25

序言：黑客帝国

1996年，英国17岁的女中学生莱安诺·拉斯特在自己所著的科幻小说《黑客帝国》中第一次使用了“Hacker”这个名词。随着计算机的普及，Hacker一词传入中国，形神兼备地被译为“黑客”，其绝妙之处就在于，仅用了两个字，就包含了“隐蔽偷袭”、“盗亦有道”、“技法高超”、“我行我素”等众多的语意，同时也宣扬了一种自由飞翔的文化格调。

黑客，一个神秘而又充满诱惑的名词，既让人望而生畏、脊背生风，又让人感觉热血沸腾、惊险刺激。的确，黑客作为电子信息时代的新名词，他们是如蜘蛛人一般在网络间滑行自如、聪明绝顶的隐身之神，也是放浪形骸、为所欲为的害群之马，他们是光天化日之下的侠义盗，也是孤独寂寞的夜归人，他们来无影去无踪，在正义与邪恶之间演绎着双重身份，国家有难之时他们会奋不顾身、挺身而出，也会一时兴起玩上几把恶作剧；他们颠覆教条，却也维护公平；他们视网络为无物，却也恪守自身的游戏规则；有时是劫富济贫的罗宾汉，有时又是巧取豪夺的剪径贼。人类最原始的好奇心和求新欲常被某种理念激活，黑客们除了和你我一样流连于普通的网络之上，更执着于另一个新天地，在这个相对自由的世界里，所有的规则被重新制定，并刻上独一无二的印记。这些人中有的最终成为背负正义之剑的侠客，有些人则沉迷其间，沦为罪恶之神。

在互联网还没有大规模普及之前，计算机病毒是最让人热血沸腾的研究热点，而随着网络的普及，黑客则被推到幕前成为聚光灯下的显赫人

物，计算机病毒和黑客攻防都代表着计算机界最高端的技术，病毒的制造者每一个都如过街老鼠般臭名昭著，而黑客则与之有天壤之别，显得另类、激昂，颇具侠客之风。

正因为黑客技术一直掌握在少数计算机精英级的人物手中，所以这样一群神秘人物常常被戴上超人的面纱，给人高不可及之感。其实很多时候，黑客就在你身边，也许是那个蹲在地上为了五毛钱跟菜贩子争得面红耳赤的老妇，也可能是那个衣冠楚楚拎着公文包啃着面包挤公交车的小职员，更可能是大班台后面不苟言笑的老总，或者是老总身后那个倒水沏茶的小工，他们白天打工挣钱养家糊口，晚上会守在屏幕前对着防备森严的网络报以浅浅一笑。这些人游移在法律与个性之间，在沉稳之中又偏偏有一丝不安分的感觉，刺激而惊险，成为让人仰视的在悬绳上舞蹈的特技演员。

一个流传于黑客网站的笑话是这样描述的：某同学买了一辆新的自行车，为防被盗，每晚用5条铁链锁将自行车锁在柱子上。一天早上，这位同学发现5条铁链锁被人打开了，但自行车安然无恙，车后还贴着一张字条：你以为学校没人开得了这些锁了吗，你认为5条铁链锁就代表着安全吗?

这就是典型的黑客行为，黑客有开锁的技能，但目的不一定是为了偷那辆自行车，他或许只是可爱的想验证一下自己的开锁技术，或者在别人的叹服中得到一种满足，这其中，有着一种强烈的自我表现欲，而这种自我表现欲的释放，才是黑客最精髓的内涵之一。

每一个自称黑客的人都对自己的技术充满信心，“高超的计算机技术”是黑客字典中永远不可能剔除的定义项之一。凭借这些貌似无所不能的黑客技术，他们有的面露微笑地躲在暗处，成为独孤求败式的神秘人物，有些则端坐于市井之间，手中握着一把柳叶弯刀，李寻欢般的不苟言笑，轻易不出手。无论哪种表情，只要他是一名黑客，就天生地包裹在一层掩饰不住的锋芒之中，让围观者瞠目结舌、哑然失声。

中国著名的黑客组织“中国鹰派联盟”的声明中说，“就好比一个人学会了武功，在没有打人之前，你不能说他是个坏人，如果他把自己的本事用来除暴安良，他就是侠，如果用来打家劫舍，他就是盗。”

黑客，离我们很近，也离我们很远，黑客精神是互联网精神的一部分，而互联网精神是“开放、平等、协作、分享”，一个真正的黑客，其实就是一个掌握着计算机前沿技术、极富创造力和正义感并积极践行互联网精神的人，我们赞赏那些富有创造力和想象力的人，如Android智能手机系统的设计者安迪·鲁宾、Linux计算机操作系统的发起人理查德·斯托曼以及诠释“身残志坚”真正意义的江民杀毒软件创始人王江民等，他们都是发明家、编程专家和网络安全专家；同时，我们也极端鄙视那些凭借一两种入侵手段就肆意侵入他人电脑，窃取他人隐私的人，他们不是黑客，只配与窃贼为伍！

真正的黑客身上有着中国“侠”的精神，身怀绝技，肩担道义。在本书中，我们要将真正的黑客与凭借计算机技术的“鸡鸣狗盗”者区分开，二者有着天壤之别，希望读者在阅读本书的时候也能对黑客其人其事有一个正确的认识，能将自身卓越的计算机技术运用在创造更美好的信息化生活之中。

目录

——第一章——

斯诺登的麻烦和整个世界的麻烦：棱镜计划

我不想生活在一个拿着高薪却实施监视别人的一举一动的世界里，也不想同样被别人监视着我的一举一动。

——爱德华·斯诺登

1 “绑匪阿瑞雅”

“这是杰瑞肖一连串的购物记录，兴趣爱好，以及各种用来定义你个性的数据，我们监控每一个社交网络、上网日志、即时消息和文字短信，你的同事、朋友、伴侣，电子邮件、手机通信记录，我们还利用保安摄像头，随时采集有价值的信息，使用这些数据，我们架构了一个几乎覆盖地球的个人特征库，我们知道你是谁，我们无处不在。我的美国同胞们，为了组织一个更完善的联邦，树立正义，保障国内安全，建立强大的国防，各节点的下载数据，都被汇总到指令中心，并接受所有被认为是有价值的问询和盘查。”

上面的文字来自2008年美国电影《鹰眼》，影片中的主人公其个人信息被监控，并被一个叫做“自动侦测智能整合分析系统”（阿瑞雅Aria）“绑架”的故事。这个被称作阿瑞雅（又名“鹰眼”）的分析系统是美国

为配合反恐行动制造的超级电脑，它可以通过各种手段收集相关事件的海量信息，并做出分析判断。而为了防止作为美国三军统帅的总统有危害国家安全的行为，这套系统的AI甚至可以自行做出判断，并对总统本人下达攻击指令。影片开始，“鹰眼”对美国军方袭击一伙被判定为恐怖分子的人给出了取消攻击的指令，但总统却执意行动，不幸引发了新一轮恐怖袭击。“鹰眼”由此认定总统危害了国家安全，总统及其幕僚应当被铲除。为了铲除总统，“鹰眼”设计了一个精密的刺杀计划。这台超级计算机为了控制作为“棋子”的男女主人公，通过各种渠道严密地监控他们的一举一动，包括他们的银行卡信息、门牌号、家庭信息、工作信息，甚至动用了每条街角的治安监控摄像头。

如此严密的监控，美其名曰“反恐”，其实可能造成更大的恐怖。信息科学的发展使得对各种隐私信息的获取变得易如反掌，而对这些信息的梳理、统计和分析之后，的确可以对世界和平起到不可估量的作用，特别是对于犯罪取证和定罪，这是提取证据的最佳手段。而在使用者不知情的前提下监控电子邮件、往来银行款项甚至你在何时何地，在哪家超市买了几元钱的烟都一一记录在案并作为未来可能有用的呈堂证供，这种为了维护正义而收集个人隐私的行径是否合法？是否在打击着和谐社会的道德底线？

似乎没有谁能给出一个两全其美的答案。

《鹰眼》只是个科幻电影，不过按目前的发展趋势来看，任何科幻都可能化作恐怖的现实。科学家和政客说科技能拯救我们，而更多的人则认为恰恰是科学毁了我们，虽然科学一直都是出于善意，但显然采取的方式有待商榷。

科学正自作主张又自作聪明地以自己的意愿极力解决的那些问题中，有一半可能是它自己造成的，它把一个大同世界分割成钻石般越来越小却看似越来越剔透晶莹的小块，就为了寻求一种各自为政的所谓平衡的价值，可结果却发现了更多无法预知和解决的超级问题。

操纵科学的是人。或者说，世界上所有的混乱中，科学并不是罪魁祸首，而用科技制造混乱的人才是。

❷ 硅谷巨头面临信任危机

硅谷，美国最大的高科技基地，垄断全球85%以上的电子芯片产业技术，这里有响当当的英特尔、惠普、思科、苹果等大公司，是天下无双的高科技电子产业群。如果硅谷停电一天，几乎等于全球信息产业停电一天。

就是这样举足轻重的科技高密集区，最近却遭遇了有史以来最严重的信任危机，几乎所有的人都深受震惊，用提防窃贼的眼神盯着这些往日不可一世的业界巨头。

可以相信，现在的人们都过分依赖网络、手机、E-mail甚至Facebook上的交流，而当最基本的网络隐私和信任都失去的时候，安全感的缺失会让整个世界大乱。

这次世界真的乱了。

阿桑奇的维基解密是建立在维护弱者正义的基础之上的，在这一点上，阿桑奇是个顶天立地的英雄。继阿桑奇之后，另一个叫爱德华·斯诺登的年轻人又挑开一层面纱，而面纱背后的真相让整个世界大惊失色。

2013年6月5日，英国《卫报》刊登未署名文章，声称美国国家安全局（NSA）要求电信巨无霸Verizon公司每天需按NSA列出的名单上交一份涉及众多政界、商界知名人士和被怀疑有犯罪倾向用户的通话记录，涉及人数达数百万之巨。这些数据将作为公职人员职业操守的证明和犯罪人员的犯罪取证；一天之后，美国《华盛顿邮报》又投下重磅炸弹，声称在过去6年时间里，美国国家安全局和联邦调查局（FBI）曾以政府的名义要求微软、谷歌、苹果、雅虎等九大IT产品供应商对其开放服务器接口，并

通过这些接口合法进入到全美网络服务器中，由此监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。或者换句话说，任何美国平民，或经由美国网络服务器的电子邮件，或是哪怕一个来自越洋电话的问候，都有可能成为被监控的对象，包括每一部苹果手机的通话，都有可能被监听。

硅谷危机让整个美国社会哗然。国会给出的理由是“这是出于对美国国民安全的考虑，从而实施的政府监控举措的需要”。

“9·11”恐怖袭击事件是布什政府永远的痛，即便是好了伤疤也一样。“9·11”恐怖袭击事件之后，整个世界在美国眼里都是不安全的。草木皆兵的美国于是开始在世界范围内对其认为有恐怖倾向的国家和组织进行尽可能的信息监控，当然，其监控的重点放在处于美国境内，但不属于美国国籍的“敏感人士”。

两天后，美国总统奥巴马的新闻发言人做出书面回应，坦诚美国政府的确正在实施着这样一个行动，而该项行动“事实上已经实施了十年之久，从‘9·11’恐怖袭击事件之后便立即开始”，但此新闻发言人强调，这一项目不针对任何美国公民并且得到了国会的授权，“符合美国民众对自身安全的迫切需要和当务之急，并置于美国外国情报监视法庭的监管之下。”

2013年6月9日，英国《卫报》刊登了对此次被美国政府认为是一级机密文件泄露事件的主人公的专访，应其“本人要求”公布了这个被网络称之为英雄、“阿桑奇第二”的告密者的身份。爱德华·斯诺登，现年29岁，美国防务软件和相关事务承包商博思艾伦咨询公司的一名高级信息员，在为博思艾伦咨询公司工作之前，有四年为美国国家安全局工作的经历。

“从良心和道义上，我无法允许美国政府侵犯全球民众隐私和互联网自由，同时我为自己也成为这个项目的其中一员感到羞愧。”他在专访中说，阿桑奇在两年之前就已经公开宣称Facebook项目之所以能在短短数

年内成为世界第一实名交友网，其最原始的推动力就是美国政府，这个政府以提供迎合大众的精神鸦片来迷惑世界，使全世界的人都甘心情愿地在Facebook上公开自己的姓名、隐私甚至今晚的晚餐和明天即将出游的目的地，可以说Facebook本身就是一个超级间谍。阿桑奇本人认为谷歌、雅虎等世界知名网络公司都专门为美国情报组织建立了专用的登录界面和后台查询系统。“阿桑奇的证据是间接的推断，而我是直接的证据，因为我亲自参与其中。”

在这两份报告中，斯诺登现身说法，并详细地列举了美国政府这一耗资巨大且影响广泛的行动的具体细节。在美国国家安全局的秘密档案中，该计划被称作“棱镜计划”（PRISM），这是由美国国家安全局自2007年开始实施的国家级绝密电子监听计划，该计划在五角大楼内部被命名为“US－984XN”。

据斯诺登提供的资料显示，棱镜计划不仅由雅虎等世界最著名的网络公司提供相关的用户数据，而且已实施长达七年之久，年成本2000亿美元。“不仅大量消耗纳税人的金钱，还一手造成了繁荣的网络世界最严重的信任危机。事实上‘9·11’恐怖袭击事件已经将整个世界裹挟在美国的反恐浪潮中，但不论奥巴马政府如何强调这是反恐的需要，这个耗资巨大的监听、监视项目都是在道德底线上刺激并侵犯公民的基本权利。”《华盛顿邮报》称，“该计划几乎没有任何的法律监管，这位总统以承诺消除发生在2013年前的恐怖事件带给美国人民的恐慌而成功入主白宫，却又在斯诺登的揭发下再次让美国民众失望。”

一石激起千层浪。斯诺登公开棱镜计划后两天，奥巴马就公开承认了此计划的存在。随后让人称奇的是，几乎所有被列在名单之中的网络公司，都矢口否认自己成为该计划的参与者和技术提供者。

谷歌CEO拉里·佩奇和首席法务官大卫·德拉蒙德在公司官方微博上声明谷歌公司从未加入国家安全局实施的代号为“棱镜”的计划，也没有为任何官方技术人员和军方侦测机构提供任何的“技术接口”；Facebook

总裁扎克伯格也在Facebook上向民众澄清了自己的无辜。“Facebook从未参与过任何为美国政府及其他国家政府提供服务器直接接入服务的项目，我们也从未收到过任何来自法院或政府机构要求提供相关信息及元数据的法令或请求，报道中Verizon公司[①]收到的请求我们从未收到过，我们此前从未听说过‘棱镜’计划。”

美国国会众议院情报委员会主席麦克·罗杰斯在记者的采访中说，从Verizon电信公司收集电话的通话记录是受美国法律保护的，而棱镜计划则报请并得到了国会的批准，并不是奥巴马政府滥用权力，“国会代表着全体美国国民，国会通过，说明代表全美民众的心声。”

但是事实上，当奥巴马坦诚说出棱镜计划的确存在那一刻起，整个世界的良心都被刺痛了，因为谁都不敢想象，你正在使用的苹果手机和iPad等设备上的所有通话和聊天记录，都有可能成为美国国家安全局的犯罪指证之一，随时都可能会有穿制服的警察敲开你的房门并将你带走，而你也许仅仅刚在Facebook上和朋友打赌吹了个牛。

作为美国盟友的德国、英国都要求美国政府给出合理的解释，并证明两国的公民并未受到来自美国安全局的监控。工党声称此计划的披露“让英国人民感到遗憾”，澳大利亚和新西兰等国的安全机构应国民要求也被迫向美国政府致函，要求书面保证本国公民的个人信息并未受到任何网络监查。

美国政府声称未对他国公民进行监视，但东窗事发后几乎没有人会相信这个世界第一霸权国家的任何声明。想象一下，互联网遍布全球的任何一个角落，而这个看似自由的网络需要一个作为汇总和收发信息的中转服务器，世界上的每个国家、每个机构都各自拥有网络服务器，但链接着整个互联网的“最高层的服务器”设在美国，也就是说，世界上任何一条通过网络传播的信息，都有可能经过设在美国的最高层服务器，或者说美国

① Verizon是美国的移动通信运营商，目前应该是全球最大的CDMA运营商。

的这些最高层服务器至少有权力通行于设立在其他各国的服务器，并在理论上可以通过间谍手段猎取其中的一部分甚至全部信息。

美国政府全球战略上的信任度透过“棱镜”后，已经降至零点。

❸ 斯诺登的麻烦

斯诺登证明了每一部手机都可能被监听，这虽然多少有些像缺少理论根据的危言耸听，但是随处可见的各种摄像头却早已让我们感到习以为常。一些城市的公用摄像头可以覆盖整座城市80%以上的街道，随时可以追踪到某个无名小卒的行踪，治安监控几乎全方位覆盖临街单位，具有红外夜视功能的监控摄像头保证24小时开机，如此一来，如果某一位置发生了劫案，警察便可以按照嫌疑人可能逃走的路线查看相关单位的摄像头以确定其方位，或者换句话说，只要你想，你可以查到任何一个人在任何时间的去向。无疑这对案件侦破等有着不可估量的作用，但换个角度，所谓隐私却在高科技的淫威之下已经无处遁形。

而经斯诺登公诸于众的棱镜计划更是入侵到网络社会的每个人交流的信息中，从你在接通互联网的电脑键盘上按下第一个键开始，几乎所有的内容都有可能被追踪溯源。由此，斯诺登成为“揭开美国伤疤，维护公众利益的英雄”。

但是斯诺登的麻烦也由此开始。

斯诺登在2004年5月7日报名参加了美国陆军特种部队的试训，但不久就因一次训练事故而将双腿摔断，花了四个月时间进行恢复。虽然他只有高中学历，但其自幼酷爱计算机，并在高中时成为了当地一个知名的黑客领袖，因入侵包括北卡罗来纳州中央银行在内的多家政府和财政部门的网站而被学校开除，正因如此，特种部队认定这是个不可多得的人才。虽然最终因伤没能继续待在美国陆军，但是美国中央情报局还是对这个电脑天

才极为感兴趣。2007年，作为中情局的特殊情报员，斯诺登开始有机会接触一些国家级的机密文件。两年后，斯诺登前往中情局下属的NSA公司担任密码研究室的副研究员，其直接领导是美国国家安全局。

在为NSA公司服务的4年时间里，斯诺登渐渐对美国政府无限制的侵犯国民隐私感到不满。他开始有意收集相关的证据资料。在他认为“证据已经足够”的时候，他向自己的上司请假，并于2013年5月20日放弃了年薪30万美元的高回报工作，丢开女朋友和父母，以旅游签证进入香港。

当然，他没有忘记随身带着价值几十亿美元的棱镜计划相关证据资料。

在连续两家世界知名报纸公布了棱镜门事件之后，揭发人斯诺登便躲在中国香港的一家酒店里闭门谢客，并向多个第三国申请了政治避难。美国国家安全局已经展开了对斯诺登的刑事调查，按照中国香港及美国法律，斯诺登至少可以获得36项犯罪指控，其服刑期限可能高达70年。

在接受《卫报》专访时，斯诺登声称自己“地地道道地成了一个东躲西藏的贼，而我本该是一个英雄，该藏起来的是那个自称世界第一的美国政府”。在香港酒店躲藏的这段时间里，他不敢上街，用撕烂的床单把房门的缝隙塞死以防被窃听，在用电脑上网时，他不得不用被子把自己连同电脑一起罩起来防止房间里可能安装摄像头，甚至连酒店火灾警报拉响了也按兵不动。

当被记者问及他顶着叛国大罪这样做的动机时，斯诺登说：“我不希望生活在这样一个毫无秘密可言的世界中，良心上无法允许美国政府侵犯全球民众的隐私，并给开放、自由、公正的互联网抹黑。美国政府也许会最终找到我并把我关进大牢，但我的良心还是让我对此举无怨无悔。我不畏惧、不后悔，你不可能在对抗全球最大的情报机构的同时不被关进监狱的风险。如果他们想抓到我，我想那只是时间问题，而我将微笑面对这一切。”

2013年6月23日，中国香港就棱镜计划最新消息的报道中说，斯诺登

已经通过合法途径离开中国香港前往第三国，其所乘的俄航SU213客机将降落莫斯科，随后蜂拥而至的各国媒体并未见到斯诺登走下飞机，俄文报纸《生意人报》在其报道中称，机场等候斯诺登的有厄瓜多尔大使馆的车辆和俄罗斯联邦安全局车辆，而后者的前身正是冷战时期大名鼎鼎的“克格勃”。但斯诺登的最终目的地可能不是俄罗斯而是厄瓜多尔或冰岛，而随后斯诺登并未在莫斯科出现，目前下落不明。据6月25日《卫报》透露，斯诺登以阿桑奇为前车之鉴，将自己尚未公开的棱镜门的相关机密文件分作几份保存在几个最值得信赖的朋友手中，一旦自己被美国当局抓获或是引渡，这些文件就会被相继公布，而这些文件的公开是美国政府最不愿意看到的。

2013年7月1日，斯诺登正式向俄罗斯提出政治避难请求。

面对世界级的恐慌没有一个国家可以坦然接受这个事实，无论是美国及其盟国，还是其他国家。

以美国为首的西方联盟声称为了“反恐”大计，一切都在所不惜，而谷歌等在“棱镜门”事件中被点名的公司也纷纷拍着胸脯替自己喊冤。德国、英国、法国等国虽然唯美国马首是瞻，但却在拥护美国决议的同时声称本国公民的所有信息都是“绝对安全的”，大有掩耳盗铃之意。

众所周知，全球的巨型网络服务器大多位于美国境内，无论美国如何否认，至少在技术和可行性上，美国都有着得天独厚的条件，使其可以“拿到任何他们认为有价值的信息，就像在自己家的后花园里抓蝴蝶一样简单”。斯诺登是一个美国情报部门的人员，他所揭露的也正是美国政府对包括别国的网络信息的窃取行径，“棱镜”折射出的光线使得躲在暗处窥视全世界隐私的美国政府彻底曝光，美国政府指控他国对其发动的“网络战”，无疑是美国政府率先挑起的，其经常摆出的一副受害者面孔，今天来看也是一场“黑色幽默”。

斯诺登及其揭露的“棱镜计划”，让美国政府在全球战略上处于完全被动，在盟国面前也是颜面扫地。

“棱镜项目不针对美国公民，就应该针对美国以外的他国公民吗？”“监控有助于反恐，于是所有人的隐私都应该为反恐无私贡献吗？”“如果反恐是一切监控手段的理由，那么是不是只要世界上恐怖主义一天不消失，全世界人民的隐私就一天得不到保障？”太多的问题随着斯诺登的爆料浮出水面，这个29岁的年轻人究竟是国家公敌还是罗宾汉式的英雄？在美国政府看来，斯诺登携带政府机密出逃他国，仅此一点就应受到叛国罪论处。但另一方面，斯诺登的行为也给全世界人民提了个醒，乔治·奥威尔《1984》中描写的“老大哥”离我们并不遥远，他正站在一个阴暗的角落窥视着人们的一举一动。

“棱镜门”事件之后，美国的一项民意调查表明，53%的美国人不支持以反恐或是其他理由获取他人的电话和网络记录；另有38%的被调查者认为无论以什么样冠冕堂皇的借口监听没有实际犯罪证据的个人隐私，都是不正确的和不能被接受的。

“棱镜门”意外地让普通民众对神秘的情报世界得以反观，在信息爆炸的时代让人们重新审视个人信息的价值，对信息的监控与控制有了新的认识。

【黑客知识】

史上各种政府级绝密信息被揭发的“门事件”：

“棱镜门”重新让人们开始审视个人隐私，也让人们重新认识和有理由回顾那些历史上著名的“门事件”。

水门事件：美国政治史上最著名的丑闻之一。1972年美国总统大选中，为了取得民主党内部竞选策略的情报，共和党党魁尼克松的首席安全问题顾问詹姆斯·麦科德（James W.McCord，Jr.）等5人潜入位于华盛顿水门大厦的民主党全国委员会办公室安装窃听器并试图偷拍相关竞选文件时当场被捕。尽管尼克松

一再声称自己事先并不知道水门事件，完全是詹姆斯·麦科德的个人行为，但在随后的相关调查中，尼克松的谎言不攻自破，并于1974年8月8日宣布辞职，从而成为美国历史上首位主动辞职的总统。而尼克松在下野后公开宣称，从罗斯福总统时开始，每一个总统都是这么干的，这一切也都是“为了国家安全，是合法的和有必要的”，但这些言辞非但没有增加美国民众对其好感，甚至将整个美国推入了信任危机之中。

文件门事件：越战在美国历史上是仅次于第二次世界大战的一场高消耗的战争。在长达十年的战争中，美军伤亡惨重，深陷越南无法抽身。这场“拔刀相助”的战争也把不可一世的美国政府拖入了金钱、人力消耗的无底洞之中，国内民众对政府和军队的支持率也一落千丈。越南战争可以说是美国历史上最不得人心的战争，它不像二战那样被认为是一场正义之战。

1971年6月，《纽约时报》等报纸相继披露了美国国防部在越战中的绝密文件。据说这些文件的提供者是一名叫丹尼尔·艾尔斯伯格的国防部官员。这批档案所提供的数据表明，美国政府从加入越战开始就已经采取蒙蔽、虚报战况和战因、战绩等欺骗手段以获取国人对越战的支持，致使花去高额的军费和近四万名美军的阵亡。档案被披露之后，全美反战情绪高涨，联邦政府名誉扫地。美国国家安全局曾以“泄露国家机密”等罪名起诉艾尔斯伯格，但美国法院最终宣判艾尔斯伯格无罪。

伊朗门事件：1984年到1985年期间，经常发生西方各国驻黎巴嫩的外交官员和记者、教师、旅游者被绑架的事件，其中有据可查的美国公民至少七人。美国经过相关侦查，断定真正制造这些绑架案的组织是伊朗的“伊斯兰解放运动”。1985年9月3日，美国国家安全事务助理麦克法兰与伊朗方面磋商，达成了以军火换人质的协议。而负责此事的政治军事处副处长诺思中校却在美国国防部的授意之下，将这些表面上卖给伊朗的军备转卖给尼加拉瓜的反政府武装。

1986年11月2日，黎巴嫩《船桅》周刊披露了麦克法兰的秘密伊朗之行和武器买卖协议的达成，两天后得到了伊朗议长拉夫桑贾尼的公开证实，美伊秘密交易武器案随即大白于天下。截至11月初，美国共对伊朗进行6次军火销售，金

额达3000万美元之巨，武器包括雷达、飞机和导弹等高尖端武器，为此3名人质获得自由；同时美国司法部的调查结果证明，国家安全局违反国会禁令，把售伊武器及相关款项转交尼加拉瓜反政府军。虽然里根政府声称对此事一无所知，但此届政府的声望和国民信任度急剧下降。11月6日，里根总统召开记者招待会，承认政府在这一问题上的“判断失误和玩忽职守”，麦克法兰辞职，诺思中校则“因犯有私自篡改、转移、销毁文件，妨碍国会调查等12项罪名”被革职，诺思被判3年徒刑，缓期执行，并处以15万美元的罚金。

伊朗门事件以替死鬼诺思的牺牲作为终结，里根政府虽然暂时渡过难关，但危机四伏的里根政府不久之后也寿终正寝。

——第二章——
会越狱的苹果

可以的话我想和乔布斯面对面聊一聊。

——乔治·霍兹

1 与乔布斯掰手腕

目前最受追捧的个人电子设备是什么？你的回答若是苹果公司的iPhone和iPad，那你就out了。至少回答不精确，精确的回答应该是，经过越狱的iPhone和iPad。

2007年1月9日，苹果公司和Cingular电信公司推出了让世界为之侧目的苹果iPhone手机，2007年6月29日正式在美国上市，由于苹果计算机一直以人性化与易用性著称，到了搭载MacOS X系统的iPhone，这些优点统统被继承并发扬光大。iPhone的接口、操作、功能与概念全部是划时代的，互动性、人性化与运行的速度都让人惊讶，手机版的苹果电脑iPhone，让整个世界为之尖叫。

作为当今全球第一大手机生产商、第一大PC厂商，苹果公司始终以极具个性的产品和超强的稳定性引领着世界电子科技的潮流。2012年3月，在iPhone和iPad销售激增的带动下，其市值令人惊讶地突破了5000亿美

元，成为电子界当之无愧的龙头老大。

其中，除了硬件销售的利润之外，苹果公司的iTunes商店也收入不菲，这个电子商店经营除iPhone自带的软件之外的第三方软件。iPhone中附带着很多试用版的软件，当用户觉得这些软件功能不错的时候，若想进一步使用，对不起，打开你的荷包拿钱来买。

电子设备及设备中的操作系统，是有版权保护的，其中包括系统中的某些收费软件。生产商为了稳固自己的经济收入，常常给自己的电子设备事先安装相应的软件，并设有使用权限，例如不允许未经许可的用户使用超级用户权限，和某些收费软件在功能上的限制使用。

这让很多人感觉不快：花了购买手机的钱，功能还要受到限制。特别是当用户购买了昂贵的苹果产品后，发现系统中有些软件删不掉，强行霸占着系统空间，浪费网络流量，拖慢整个系统的运行速度；还有些非正常渠道的软件安装不上，或者虽是正版软件，却因收费而限制了大部分功能；甚至用苹果手机拍照时，总是会发出一声蹩脚的咔嚓声，虽然不影响使用，却总是感觉很心烦。

目前世界上的智能手机所采用的操作系统及核心技术基本上被几大巨头公司垄断，Apple的iOS、Nokia的Symbian，以及Google的Android，每种操作系统互不兼容，就像中国的联通和移动，虽然都是经营无线通信，却始终貌合神离不可融合。与苹果手机的操作系统不同的是，Symbian系统和Android系统除了不允许用户擅自删除系统程序之外，用户权限还是可以满足一般使用的，而在苹果公司的iOS中，用户权限极低，并且只能安装和使用经苹果商店售出的应用程序。如此给用户带来的好处倒也是显而易见，苹果系统极难被病毒攻击、稳定性强、省电，几乎从不死机，除了造就苹果的经济利益之外，更打造了苹果坚如磐石的口碑。

用户权限这把“双刃剑”的另一面就是，苹果的手机不能随心所欲地将界面个性化，不能删除系统自带的应用程序，不能使用第三方输入法甚

至是非iTunes平台上的第三方软件。

用过计算机的人都知道，Windows的使用者可以随意更改系统桌面和图标，给一成不变的系统以视觉上的常用常新感。那么，在功能如此强大的苹果手机上，一些最基本的功能都无法使用，这不能不让人感觉别扭。

就在苹果公司推出第一台苹果手机仅仅两个月后，一个注定要扬名立万的小伙子出现了，只看名字，简单普通毫无出奇之处：乔治·霍兹（George Hotz）。

最初的iPhone是以AT&T合约手机的形式发布的，即iPhone用户只能使用AT&T公司的无线终端网络进行通信，而当时才17岁的霍兹是T-Mobile的用户，只是一不小心，他不明就里地买了台iPhone却无法使用原来的电话卡，于是天才的霍兹突发奇想，开始研究手上的这台iPhone。

霍兹面临的问题很像赵本山小品里那只会下蛋的公鸡，不是它的活要让它干，这多少有些异想天开，而霍兹和所有同龄的年轻人一样，对每一件有挑战性的事情都跃跃欲试，而让一台机器运行根本就不该它运行的功能，无疑非常刺激。或者换句赵本山式的说法，霍兹天生就有做公鸡中的战斗机的特殊本领。

智能手机与普通的电脑工作原理大同小异，无非是用CPU去接收和处理数据，然后转到相应的软件来运行它。而破解这部手机，关键就是找到一个方法，让手机的基带处理器能识别霍兹的指令，从而达到目的。

霍兹翻烂了手机的说明书，然后把手机拆开，按照在学校里学到的电工知识和网络上的相关介绍，试着在基带处理器上焊进一对电线，然后用一个5V的电流接通基带处理器，如同催眠一般扰乱了基带处理器的运行频率，之后他为这台破解机写下一个程序，使其可以正确识别任何运营商的无线电话卡信号并自动接收转入相应的处理程序，从而实现了霍兹的意愿。

在两个同学的帮助下，霍兹用了近一个月的时间，在搞坏了三台手机

之后，终于达到了目的。8月27日后半夜，霍兹把自己的T-Mobile电话卡插到这台经过自己改装的iPhone电话上，然后给远在日本的姑姑拨通了电话，“声音出奇地清晰，姑姑甚至说她听得到我激动的心跳。”

听到心跳显然有些夸张，但不可否认，也可以想象到电话接通的一瞬间，对于一个17岁的男孩子来说，这应该算是人生的第一个辉煌了。

接下来，霍兹架好了摄像机，坐下来重新打开一部新手机，记录下改装的整个细节，然后他满怀豪情地把这段视频传到了网上。全球首台破解版iPhone的制作视频很快就吸引了200万的访问量。

媒体哗然。“青年才俊击败苹果帝国”，仅这几个字就足够了。第二天，世界排名前十位的新闻网站头条上，都赫然地打上了“乔治·霍兹”几个大字。随后，位于肯塔基州路易斯维尔市的手机修理商CertiCell联系了霍兹，在与霍兹的这笔交易中，CertiCell用一辆尼桑350Z跑车和3部8GB 容量的最新款iPhone弄到了霍兹写到手机中的那段程序的源代码。

在经过霍兹如此这般的改造之后，iPhone不仅可以使用所有的电话卡，还可以下载和使用任何可以运行在iPhone上的软件，最重要的是，它打破了苹果公司对iPhone的限制，连软件的使用都可以是全功能并且免费的。

霍兹在接受CNBC电视台记者采访时说：“可以的话我想和乔布斯面对面聊一聊。”显然大忙人乔布斯对这个提议是不会有兴趣的。

美剧《越狱》热播后，给手机打开用户权限的这种操作也被冠以“越狱”，形象生动而充满了刺激。

❷ PlayStation 3的噩梦

霍兹无论如何都可以算作一个天才，即便他没有破解iPhone。他编写的第一套电脑程序是一个小小的提醒记录程序，以便让电脑随时提醒

自己一些重要的日程，这种日程提醒程序并没有多少难度，但是对于一个只有5岁的小孩来说，则另当别论；14岁凭借自制的测绘机器人入围英特尔国际科学与工程大奖赛（Intel International Science and Engineering Fair）决赛，两年后又把一套脑电波控制系统搞得有模有样。要知道，类似的系统，很多知名的电子公司也不知道从何入手，就在他破解了iPhone后不久，他又再次入围英特尔国际科学与工程大奖赛决赛。“我是天生的黑客，我不是因为某种理念而成为黑客，而是因为我无聊。破解就是和系统进行较量，我在和硬件原作者进行较量。当破解进入一台电脑系统时，我感觉自己充满了血性。”

2009年12月26日，霍兹在自己的博客中写下一句没头没脑的话：“是时候了！”而一些霍兹的铁杆粉丝则感觉到了其中另有深意，当粉丝们反问的时候，霍兹自信满满地回复：“我要挑战一个更有难度的玩意儿，就是那个号称铜墙铁壁、坚不可摧、傲立三年未遭破解的索尼旗舰之作PlayStation 3。”

众所周知，索尼公司的PlayStation系列游戏机（以下简称PS）是世界通用的权威游戏产品，其核心代码是国家级机密。在这个产品中，用户被严格限定了软件功能的拓展，索尼公司在说明书中明确标明，所有的游戏软件必须在指定的网站下载并付费后才可能被系统接收，与iPhone一样，这一点让几乎所有的用户恼火而又力所不逮，只能听从索尼的摆布。

霍兹的这一次挑战迎来了众多的瞩目，其中无数粉丝擂鼓助威，也有索尼公司的相关人员静观其变，只是这一切似乎都改变不了霍兹的决心，“我就是要干掉它。”

接下来的几周时间里，霍兹足不出户，把手头的几台PS机拆得七零八落，并强硬地在系统中植入了一个新的程序，这段程序因为过于庞杂，他不得不又为PS机扩展了内存。一个半月之后，头发零乱、满眼血丝的霍兹终于出关了，他在间断了许久的博客中放上了新的一句话：“请起立，为我鼓掌。”

掌声如雷。

有粉丝回复他：“我以为你死了，或者因为失败而逃跑了。”霍兹回复了一个笑脸图标：“伟大的霍兹，是不死的芬尼根[①]。”

为此他特地在破解之后的PS3启动画面上，加入了《芬尼根的觉醒》这本书的封面，这种经过“越狱”的PS3，也理所当然地被称作“芬尼根PS3”。

索尼公司第一时间截获了破解后的PS3，并为系统制作了专门针对破解程序的升级补丁。但霍兹显然把PS3的核心代码研究得比索尼公司的技术工程师更通透，每一个针对破解版PS3的官方补丁出现之后，过不了多久，霍兹就会推出新版的破解程序，并且在随后的不断精研中，霍兹掌握了PS3的底层密钥，也即现在人们常说的Root Key权限。

为了彻底打败索尼，霍兹这一次并没有把破解程序拿来换钱，而是连同破解教程一起发到网上供全世界的PS3用户免费分享，这样的“芬尼根PS3”不仅可以卸载原有系统，还可以玩盗版游戏，霍兹用一段不足1000行的代码打垮了索尼，让索尼游戏商店这个索尼计算机娱乐公司力求打造的支柱产业颗粒无收。

日本人很愤怒。相比苹果公司的沉默应对，索尼公司则在绝望之下以违反“联邦反电脑欺诈与滥用法案”（Computer Fraud and Abuse Act）并侵犯了公司版权为由，一纸诉状将霍兹告上了法庭。

霍兹的粉丝们，包括那些不得不为自己的PS3游戏机购买正版游戏软件的使用者当然都站在霍兹一边，认为霍兹在捍卫信息自由和维护世界性的信息共有权，认为索尼愚蠢地剥夺了消费者对已购得商品的处置权，是霸王行径。而索尼则在公诉状中声称霍兹的行为不仅侵犯了索尼的注册版权，还引导消费者进行游戏作弊，同时对已经付费购买正版游戏的消费者也构成了侵犯，试图拉上那些掏了钱包的消费者站在自己一边替索尼说

① 《芬尼根的觉醒》是乔伊斯最后一部长篇小说。内容是有个搬砖工人芬尼根从梯子上跌落，大家都以为他死了，而他却安然无恙。

话。事实上，那些花钱购买了游戏软件的消费者，出于不再继续为新游戏掏钱的目的，也一哄而上跑到霍兹阵营中去，索尼公司孤立无援，霍茨这边却锣鼓喧天热闹非常。

最终法院还是支持了索尼公司，判决霍兹不得再对索尼的产品进行破解或是传播破解信息，同时索尼还有权监控霍兹在互联网上的个人账户变动。更重要的是，索尼有权获得使用“越狱”PS3观看和下载视频者的IP地址。

这无疑让所有索尼PS3的使用者个人隐私暴露无遗，判决仅凭这一点便足以引起海啸般的众怒。

❸ “从良”

Anonymous一向是“教父级”的黑客团体。其成员遍布世界各地，高层人员相对固定，且手法高超，维基解密事件[①]中曾为阿桑奇摇旗呐喊，并大肆攻击政府网站且频频得手，一时间抢尽了风头。

在霍兹与索尼的对决中，Anonymous自然不肯坐视。2011年4月4日，Anonymous在网上公开声明，声称对日前Sony.com和PlayStation.com被黑事件负责，并发布了索尼高管的私人电话号码及家庭住址等信息，组织并号召抗议者对索尼工作人员进行人身骚扰，同时要求索尼公司放弃一切针对破解PS3的诉讼。

霍兹独自面对世界最大的电子设备制造商索尼这一事件本身就充满了传奇色彩，颇有些武侠小说中无名小辈挑战大门派的感觉，本来就足够吸人眼球了，Anonymous的加入更是推波助澜，事件向着白热化发展。

2011年4月19日，索尼公司的四组服务器被非法入侵，近亿用户的个

① 有关维基解密详见本书《E时代X档案——阿桑奇和他的维基解密》一章。

人信息数据泄露，包括密码、生日、邮箱和居住地址等个人信息，其中还包括一部分用户的信用卡数据等金融信息，索尼为此不得不暂时关闭服务器并进行系统改造和升级，为此索尼每周的损失达到惊人的1000万美金。

黑客行为本身就有着群体性。与Anonymous组织一样自告奋勇的世界级黑客组织LulzSec，也在4月中旬入侵了索尼电影公司（Sony Picture）的中央服务器，成功地盗出了一百多万份用户密码，并在网上发布消息，公布索尼电影公司中央服务器的后台入侵方式，号召广大黑客到索尼的服务器去“各取所需”。

在这两大黑客组织的引领和教唆下，各大黑客组织和个人纷纷出动，打着劫富济贫的旗号肆虐网络。日本知名的游戏机制造商任天堂（Nintendo）、世嘉（Sega）都未能幸免，而艺电（Electronic Art）、新闻集团（the News Cooperation）、博思艾伦咨询公司（Booz Allen Hamilton）、北约（NATO）等非日本的游戏厂商、新闻机构、商业公司和政府机构也遭池鱼之祸。

“他们最开始只是为了捍卫网络自由，却刮起这片腥风血雨。”面对一片混乱的网络世界，霍兹表现出彻底的无奈，“我认为黑客只是一群有着电脑技术的人，而技术是无罪的。”在与Anonymous和索尼公司各方面多次商议之后，2011年4月29日霍兹公开了一份声明：

“我，乔治·霍兹，向来做事光明磊落，从不做违反江湖道义的勾当。对于Anonymous的行为我表示极不认同，也希望索尼别把这笔账算在我的头上。创造和探索是美好的，但即便是对待索尼这样的小人，盗窃也是最可耻的行为。你们在给黑客的名字抹黑。”

与Anonymous和LulzSec两大黑客组织划清界限的同时，在压力的面前，索尼与霍兹达成了和解。索尼公开宣布放弃对霍兹的一切起诉，而霍兹终身不得染指索尼产品的技术保护措施。索尼甚至自降身份，邀请霍兹到索尼公司位于美国的总部，请他为PS3的工程师们讲课。

但是显然这一纸和约只对霍兹和索尼双方有效，霍兹的粉丝们依旧表

现出最彻底的不妥协。每天依旧有为数众多的人聚集在索尼的门店前进行示威，向索尼标识上吐唾沫。

渐渐长大的霍兹现在看上去相当地成熟和稳重，这个后起之秀、黑客精英，在索尼事件之后消失了近一年的时间，据消息灵通人士透露，世界最大的社交网站Facebook将霍兹招至麾下，成为该公司网络安全的领头羊。

“Facebook是个好地方，有效率，很年轻。不过我可能不会做太久。至于破解电子设备，对不起，我也许还会随便找个什么东西来研究一下，但是不会再把破解信息发布在网络上，在这点上我已经‘毕业’了。”

❹ 苹果中最棒的那只虫子

与霍兹一样，令苹果公司头疼不已的还有另一个天才小子，与霍兹年龄相仿，只是比他多了一脸胡子。

尼古拉斯·阿莱格拉（Nicholas Allegra），网名“Comex”，长相酷似哈利·波特。需要严肃声明的是，这个90后的小伙子是个超级苹果控，爱极了苹果公司的各种电子产品，每当有新产品推出，阿莱格拉都要第一时间弄一台回来尝尝鲜，而他尝鲜的方式却与众不同，他喜欢把新入手的机器拆开来探个究竟，特别是破解收费软件，被黑客界视为苹果产品领域内的魔法师。他9岁开始自学编程，2011年6月，19岁的阿莱格拉使用自己研发的Jailbreak ME系统将iPad2成功破解，一时间名声大噪，随后他把这串代码的改进版公布到网上，任何苹果电子产品的使用者都可以免费下载，利用它在数十秒内就可以冲破苹果在iPhone以及iPad两种设备上极为严密的技术保护，在用户欢欣鼓舞的同时，气得苹果公司吐血不止。

在霍兹事件之后，苹果公司从2008年开始实行名为“代码签名”的保障措施，这种技术手段可以随时监控用户在苹果的电子设备上运行非苹

果系统的代码和指令。此套技术措施可以在黑客找到系统漏洞并成功进入iOS系统内部的前提下，保护苹果原有系统，即只能够使用那些经苹果系统允许的软件和命令，所有非苹果产品内部指令都在这道防火墙的过滤之下被严格禁止。

“代码签名”在阿莱格拉看来显然是不堪一击的。阿莱格拉在随后发布的Jailbreak ME 30中针对“代码签名”特别改进了程序段，以便让苹果系统认为Jailbreak ME 30是合法存在于苹果设备之中的，这样一来安装了Jailbreak ME 30的iPad 2以及所有使用苹果iOS433之前版本的苹果设备都可以顺利越狱。此举迫使苹果公司在iOS433系统推出仅仅9天就不得不加班加点地赶制出iOS434，封堵了可以被用以越狱的系统漏洞，同时采用了动态代码变更技术，随机变换代码在内存当中的位置，让黑客难以查找指令并进行任何形式的破解。尽管如此，还是有超过140万用户通过这款工具对iOS设备进行了越狱，前提是只要用户不升级更新自己的苹果系统，就可以永久免费使用第三方的软件。阿莱格拉当然也没闲着，针对iOS434的改进版Jailbreak ME 30出台后，神奇般的以其人之道还治其人之身，同样以动态代码技术让苹果的反越狱代码抓不到自己的代码，两种程序在内存里打得一塌糊涂之后，最终还是阿莱格拉的程序段胜出。

“我在这上面花费了相当多的时间。我得承认，苹果公司的程序员是世界上最棒、最敬业的程序员，但是无疑我比他们还要棒一点。”阿莱格拉牢牢占据着上风，很有成就感地对采访他的《福克斯》杂志记者说。

在这场“道高一尺，魔高一丈”的较量中，阿莱格拉一个人单刀赴会，让庞大的苹果公司非常难堪，苹果公司最后不得不出了下下策，在其操作系统中将阿莱格拉程序下载网站JailBreakMe.com进行屏蔽。而此种做法，在黑客们看来无疑是承认了自己的失败，虽然封堵住了Jailbreak ME30，但在技术上却甘拜下风。

“好吧，我承认苹果公司，这个电子产业的巨无霸败给了一个乳臭未干的毛头小子。”程序安全研究员Dino DaiZovi是《苹果中的虫子》一书

的特约撰稿人，他在书中坦言Jailbreak ME程序的复杂性和技术高度堪比当年的超级工厂病毒Stuxne，并声称世界上现在还精于技术的黑客中，阿莱格拉足可以一当十，“其他黑客与之相比，技术上至少落后了五年，由此，我们有理由相信，阿莱格拉是所有苹果的虫子中，最强大的那一只”。

在美国本土，这种给手机越狱的做法是合法的，虽然很多电子业巨头曾联名申诉，要求对破解电子设备的行径处以重罚，但阿莱格拉的行为至少不是以赢利为目的，无论什么法律条款，都对阿莱格拉的做法无能为力。

“我并不是想钻法律的空子，也不想以此发家致富，事实上如果我把用来编写Jailbreak ME的精力拿出来研究随便别的什么，都可能是登峰造极的，并且可以给我带来巨大的名望和财富。我之所以这么干，只是觉得这实在太有趣了，我一个人面对一个庞大的世界级对手，并且凭自己的能力打倒他，这简直太棒了。”忘了说一句，在所有这一切都结束的时候，阿莱格拉还只是个20岁的大学学生。

鉴于阿莱格拉的高超技术和特殊身份，在采访他之后，记者在随后发布的新闻稿中，打趣地建议苹果可以考虑将这名天才少年招至公司的软件安全团队当中。随后有外国媒体评论说，“去苹果实习？六位数的薪水以及一间独立办公室怎么样？”

这倒不失是个好主意，但不知道阿莱格拉会不会屈尊为自己手下败将打工。

年轻人行事往往较为冲动，而一些黑客行为常带有侠盗罗宾汉式的感觉，在这种感觉的驱使下，黑客常常行走在犯罪的边缘，左边是天堂，右边是地狱。各大公司的版权、商业利益受法律保护，霍兹和阿莱格拉的行径虽然得到了普天下所有人的掌声，却常会给自己惹上不少的麻烦，甚至是牢狱之灾。

在霍兹与索尼的较量之中，不仅最后对簿公堂，甚至使得世界各大黑

客组织蜂拥而上，横扫日本各大网站，这些行为虽然彰显了黑客界中“所有信息都应该是透明并且免费”这一信条，却也违反了世界公约和各国法律，他们在让世界惊叹的同时也触动了法律的底线。同时会让一些同样富有激情的年轻人热衷效仿，而这种连锁效应一旦失控，就会让这些精英级的计算机技术人才遭受法律的制裁，使人才变为罪犯，这无论对个人还是整个世界都是遗憾和损失。

【黑客知识】

超级工厂病毒Stuxne：这是世界上首个专门针对工业控制系统编写的破坏性病毒，它可以同时运行在Windows操作系统和西门子SIMATIC WinCC系统中，并针对这两个操作系统中特有的安全漏洞进行恶意攻击。由于西门子公司的数控机床系统垄断着全球的数控电子产品市场，所以在钢铁、电力、能源、化工等需要用到西门子数控产品的几乎所有重要行业中，该病毒的发作都造成了重大破坏，最著名的一次是病毒曾造成伊朗核电站推迟发电。2010年9月25日该病毒首次被中国病毒联防库捕捉。

越狱的iPhone：苹果手机在出厂时，最高用户权限是“封闭式”的。作为普通用户是无法取得iOS的root权限的，更无法将一些软件自行安装到手机中，只能通过苹果专用的软件商店购买一些软件（当然也有免费的），但这种方式就把用户牢牢地桎梏在苹果的管辖范围内。

iPhone的越狱就是通过非正常手段取得系统的最高使用权限。越狱不是必需的，但经过越狱的手机对于一些用户而言，使用起来会更方便、更好玩。越狱后，能够免费使用很多软件，更能够使手机的易用性进一步增强。

魅族遭黑客攻击事件：2012年8月15日，国内新生代手机品牌魅族举行的“IQ大比拼，看谁更快更聪明”比赛。最快将十道题目全部答对的人，将获取10万元现金奖；而参加此次活动的，只要连续回答3题正确后，便可以获取300元代

金券，在官网线上商店购买魅族MX全新双核、四核即可优惠300元。活动当天魅族官网的访问量就突破400万，而这400万的访问量中有相当一部分是黑客攻击，他们绕过答题环节，直接向系统发出答对了三题的信息，让系统不停地吐着电子优惠券，与此同时，淘宝网等各大网购页面上，也用各种醒目的字眼给代金卷标价5元至100元不等，致使当月魅族的销量激增至上万台，一时劲爆非凡，由于魅族手机一炮走红，成为继金立、联想之后又一新生国产手机大品牌。

手机病毒现状：据网秦“云安全”监测平台最新发布的《2012年上半年手机安全报告》显示，中国内地以25.7%的感染比例再次成为全球最大的手机“中毒”重灾区。2012年上半年查杀的手机恶意软件数量，相比2011年下半年增长42%；感染手机1283万部，相比2011年上半年增长177%。成为除电脑之外的电子产品病毒“重灾区”。恶意软件多伪装为主题类、工具类和电子书App[①]应用进行传播，像“硬币海盗”、“电源管理”、“植物大战僵尸”等，有的就包含有“李鬼”恶意软件。

有网络安全专家指出，目前手机端应用市场与PC端相比，尚缺乏覆盖面广且有效的病毒检测与防御机制。手机病毒的侦测防范软件市场潜力巨大。

① App：英文application，应用软件。App.为其缩写，即使用在苹果iMac，iOS，及Google Android等系统上的应用软件。

——— 第三章 ———

将31亿人吸在一起的数字化海绵
Android之父安迪·鲁宾

我的好奇心和多动症促使我：如果世界上没有让我感觉足够有趣的玩具，我就自己创造一个。

——安迪·鲁宾

❶ 安卓之父

能称得起举世闻名的人，政治家如华盛顿、拿破仑、毛泽东，艺术家如梵高、毕加索，音乐家如贝多芬、莫扎特等应该排在前列。高科技领域中，比尔·盖茨、乔布斯也可称翘楚，只是很多人可能极不公平地忘掉了安迪·鲁宾（Andy Rubin）。

这世界上叫安迪·鲁宾的人也许会超过十万个，但只有这一个是金光闪闪的，他让微软公司咬牙跺脚，让苹果公司恨得胆颤，却让谷歌异军突起，成为智能电子终端市场的风向标。

如果按拥有专利数量来衡量，自称是史蒂夫·乔布斯和达·芬奇混合体的日本人中松义郎可堪称为世界头号发明家。他一生拥有3300多项专利，并且时至今日这个数字还在继续增加，但是中村博士的发明多是些

充满奇趣的小东西，比如可以降血压除焦虑的音乐高尔夫球棒等。世界上第一块数字显示的电子表的发明权也可以归为中村博士名下，只不过说实话，电子表的科技含量其实并不大，它是把已经运用多年的晶振技术与石英LED技术合二为一而已，但相比于中村，安迪的每一项发明都堪称为世界之最。

世界上第一部无线个人掌中电脑Motorola Envoy、第一个可以集成在主板上的非硬件调制解调器都是安迪灵光一闪的结果，更别说互联网多媒体电视WebTV和Sidekick操作系统了，这些都可以称得上是改变世界的发明。

当然，最伟大的是他的安卓（Android）智能手机系统。

安迪是个典型的欧洲式的60后，激昂、精力充沛，满脑子奇思怪想，只是他的低调让他似乎总是有意无意地被世界遗忘在某个角落里。但是，他为世人所熟知的却是因为一段代码，这段代码打造了一个真正在全球移动的网络平台：Android智能手机操作系统。

在孩子般的天真里打造只属于自己的玩具，并乐在其中，这才是安迪最大的快乐，他给全世界的通信界带来了一场革命，也给全球的人制造了一个老少皆宜、乐此不疲的玩具——安卓。

安卓绝对是世界通用的快乐代码，四十亿地球人，谁不知道安卓？就像用电脑的人谁能不知道比尔·盖茨呢？

❷ 安迪的黑客替身

相比于“Android之父”这个称谓，安迪·鲁宾更喜欢在自己的名片上印上“机器人专家”的名头，而不是什么“Google项目高级副总裁”或是工程师、CEO之类貌似金光闪闪的头衔。“那些钢铁结构的人形动物，才是我的孩子，它们带给我做父亲的成就感。”

6岁时，安迪自己打造了一件会自动行走的机器人，这让开电子产品公司的父亲极是惊诧。父亲的店面不大，不得不把上级制造商的样品放在自己的家里。安迪于是可以接触各种最新的电子设备，这其中包括电子信用卡的刷卡机和各种插了电有声有形的电子玩具。安迪把一只电动青蛙的电线连接在另一个机械手臂上，让那只机械手臂带着青蛙一上一下地荡秋千。接下来的几天里，安迪继续改进这只机械手臂，他拆掉了某个机器人的上半身，并给这个机器人的双腿加装了弹簧，以便让这个两条腿、一只胳膊的怪物“走起来不那么大的动静”。更奇怪的是，那只兴致勃勃的青蛙一边左摇右摆地荡着秋千，一边哼着圣诞老人的曲子。原来，安迪把一张电子贺卡的音乐芯片装在了青蛙的身体里。

“你这只是拼凑而不是创造，只有愚蠢的人才拿着拼凑的东西沾沾自喜。”虽然相对于6岁的孩子来说，这样的改造已经算得上是不小的奇迹了，但有着心理学硕士学位的父亲还是不太满意。

“可是，我只是感觉这很兴奋，让我很快乐。”小安迪似乎还想据理力争。板着脸的父亲不依不饶，“快乐是自己创造的，而不是拿着这些垃圾玩具简单地重复别人带给你的满足。如果你想真的开心，就自己去弄一个。”

可是，那真的很快乐，那些非铜非铁的电子元件在通了电之后可以发光发热自己发声，并根据设定的程序按一定的路线或动作运动，这简直太妙了。

1986年，23岁的安迪如愿以偿地从纽约由提卡学院计算机科学专业以优异的成绩毕业，他的毕业设计就是一个似乎无所不能的工业机器人，这个设计的巧妙之处在于机器人可以设定抓握力度，并在遇到阻力后立即自动停止动作，最让人称奇的是，其工作精度可以达到当时机械手望尘莫及的程度。

这让以专业生产高品质相机镜头的卡尔· 蔡司公司大感兴趣。安迪的毕业设计于是成为卡尔· 蔡司公司高精度元件的自动焊接机械手的拓展项

目，在巨额资金的帮助下，安迪仅用数月时间就把成品的高精度机器人投入到生产线上。

“只是，它还不够智能。”安迪对自己的这个设计并不是十分满意，在向公司高层递交了进一步改进机器人设计的方案里，安迪打造了一个真正由程序控制的智能机器人项目，并野心勃勃地声称，这将是史无前例的壮举。

“可是，作为相机镜头的焊接工人，它已经足够好用了。我们没有必要为了一只机械手臂投入太多华而不实的功能来哗众取宠。”

公司高层的批复让安迪很失望。作为一个喜欢电焊枪，也喜欢编程序的追求尽善尽美的人来说，只会焊接的机器人不是好的机器人，“它应该是无所不能的。”安迪开始萌生退意，在第一代机械手臂投入生产后，他请了长假。

开曼群岛风景不错，白色的沙滩和碧绿的海水很适合抚慰人心。安迪揣着他的不成形的智能机器人设计方案来到开曼群岛，每天迎着阳光，纠结于自己的未来十年中，应该按照公司的意愿继续搞那个只会操作电焊枪的机器人还是按着自己的思路完成一个超乎常人想象的智能玩具。

这天早上，当他回宾馆取他忘在房间里的太阳镜后再转回来时，沙滩上多了一个人，手上正拿着他零乱勾画的未来机器人的蓝图。

“这个，是你的想法？”

安迪点头。

“你觉得这伟大的想法是不是需要有个强大的推动力来达成它？比如，优越的薪金待遇、任你思维自由扩展，并能满足你各种奇思妙想的团队，和一间设备齐全的实验室？”

“哦，我可以得到你说的这些吗？”

“当然，来我这里吧，我的公司，名叫‘苹果’。”

1989年的苹果公司绝对算得上足够另类并且氛围非常自由的公司。在这里，没有固定的上班时间，你可以来去自由，只要按时交上你的“作

业”即可，这里你可以把各种怪点子变成现实，若是能得到上一级首肯，便会拿到高额的启动资金来达成你的想法。而这种近乎嚣张的自由，正是安迪求之不得的。

安迪得到了一间独立的办公室，四面的阳台，豪华得像总统套房，实验室里有他的专线视频电话和各种高新设备用以满足他的设计要求，当然，这一切都得益于他那个超级强悍的机器人设计图。

设计进展得很顺利，平时那些设计部的人各自为政互不干扰，周六、周日就会聚到一起讨论和交换各种新奇的想法，这让安迪很惬意，为了与其他人联系方便，安迪改造了公司的电话系统，以便“随时可以听到公司内任何一个设计人员的设计意图”。他在总台交换机上加装了一个分频转移装置，并在自己的办公桌上接上了终端接收机，这样他就可以每天像调频电台一样任意收听同事们的对话和交谈信息了。

这显然不够刺激。偶尔，安迪会通过自动留言系统给设计部的同事们发出语音留言，声称总裁斯卡利已经决定年底的分红政策；甚至扰乱门卫的电子门禁系统，发出“斯卡利总裁的车五分钟之后将抵达”的命令。

小儿科的恶作剧之后，安迪显然还不过瘾，在开发智能机器人的间歇里，他试验性地制作了几个安了轮子的小机器人，这些机器人上安装了GPS定位系统和摄像头，可以随意穿梭于设计部的各个办公室。安迪每天上班的第一件事，就是由这些机器人给自己倒上咖啡，然后他就将这些钢铁人派出去自己玩。当然了，这些钢铁人会随时发回一些安迪认为有价值的同事们的工作信息用以完善自己的设计。

他给这些机器人专门编写了程序，可以自动开关机器人携带的摄像头，然后把相关的信息通过互联网发送到自己的电脑上来。

那时苹果公司的奇景之一就是，每天都会有一个钢铁人一路呼啸地穿梭于各个办公室之间，手里或者拿着一杯咖啡，或者是几封信，而这个钢铁人被同事们冠以“安迪的黑客替身”，亲切而又可爱。

❸ 被入侵的黑客

在苹果，如果你以为安迪只会任性地搞一两个虽然出风头却百无一用的机器人那就大错特错了。事实上，苹果公司的第一台多媒体电脑Quadra系列和历史上第一个软Modem都是安迪的作品，也都是这个时期研发出来的。

而多媒体电脑的设计初衷，也不过是安迪想在未来的机器人上，集成声音和影像识别功能，没想到阴差阳错地打造了全新的多媒体电脑平台。软Modem的设计理念也不过是要把机器人采集到的信号通过小巧的无线互联网设备发送出去。

1992年，安迪的机器人计划被迫搁浅，苹果公司开始进入通信领域，并成立了一个名为General Magic的新的子公司用以专门研发手持通信设备，而安迪的奇思妙想又在这里得到了发挥。他突发奇想，要把电脑的功能整合到一部电话中去。

这绝对是个大胆而超前的想法，要知道那个时代，能把全部电脑的功能整合到一部笔记本电脑中都很有技术难度，而安迪的理想是，在硬件暂时达不到目的的前提下，在软件上完成这个设想。

这是个独一无二的手机操控界面，在这里除了拨打电话之外，安迪和他的团队还为手机设计了多媒体功能，并将所有功能整合到一个底层操作系统上去。

General Magic是个成功的手机操作系统，也是历史上第一个初具规模的手机操作系统，只是这个系统太超前了，甚至只能在模拟机上演示，硬件上根本无法实现。

这个乌托邦式的设计让苹果大为光火，投资上千万，结果弄出了这个鸡肋一样无法实现的东西。安迪和他的General Magic团队于是集体失业了。

失业了也闲不住，那些奇怪的念头总是从脑子里往外冒，把全套的多媒体功能安装到手机上不行，那就安到电视上吧。于是不出几个月工夫，交互式的互联网电视WebTV横空出世。

WebTV除了具有普通电视机的功能之外，还具有Web访问功能，增加了中央处理器和调制解调器的电视机会按照用户要求与Internet相连，查找到用户需要观看的节目和信息，在不需要互联网时又可以随时切换到正常的电视频道中。

仔细想想，WebTV其实没有多少技术含量，不过是把现成的电视机加装了互联网功能和用户点播系统，这与安迪一直努力的智能机器人的很多方面是互通的，或者说，这个WebTV根本就是安迪梦想中的机器人的另一个试验场。只不过，这个试验场恰好切入了一个合适的消费群体，居然获得了巨大的成功，成为继数字电视之后最受欢迎的娱乐平台。

1997年，微软公司收购了WebTV专利，也把安迪招至微软旗下，继续他的智能机器人之梦。

只是与苹果公司更强调个性的张扬相比，微软的严谨让安迪很不适应。他每天埋头于机器人之中，不断地扩展机器人的功能，完善其控制程序，把摄像头、语音识别、红外线等技术不断地附加到机器人上去。和在苹果公司一样，安迪每天仍是不断地把机器人放到微软的各个办公室里去游荡，只不过这一次他闯了祸。

随着机器人的功能不断丰富，控制机器人的程序也日益复杂，安迪在编写控制程序的时候难免有百密一疏的地方，结果这个可以接入互联网的机器人因为程序的漏洞而被人利用，从而把摄像头拍到的微软公司内部影像传入黑客网站上，造成了微软内部资料的泄露，甚至有黑客网站将微软公司的停车场上有几辆豪车都公布于众。

这让一向严谨的微软大为光火。于是，等待安迪的只有一个结局，带上那个钢铁人走路。

❹ 数字化海绵

失业成了习惯，安迪反倒安然了。他重新回到自由状态，这反而激发了他的热情。他开始埋下头一心一意地研究起真正的万能机器人来，同时还不断地改进电子设备的体积和运算能力，因为他发现，从设计机器人的经验上来达成一个智能化手机的想法，真的太刺激了，甚至比一个超能力的机器人更让他向往。

想想吧，除了接电话，在小小的手机上就可以与整个世界对话，五彩缤纷的互联网被紧紧地握在手上，那该是怎样的惬意?

安迪开始把智能机器人技术向智能手机全方位过渡，他成立了一家名为Android的公司，专心打造一个面向所有软件设计者的、统一制式的、开放性的智能手机操作系统平台。

Android这个名词来自法国人利尔亚在1886年发表的一部名为《未来夏娃》的科幻小说。在这本书中，那些有着人类外形的机器人被称作Android，而这正是安迪的向往所在：智能、机器、开放、包容。

几个月后，安迪拿着一个宽屏幕的手机来敲谷歌总裁办公室的门，并极其详细地演示了其功能，这让谷歌很兴奋。不久之后，安迪的名片上就多了“谷歌工程部副总裁”的头衔，继续负责Android系统的进一步研发。2007年11月5日，谷歌公司正式推出其第一代智能手机系统，那个小巧可爱的绿色机器人形象成了Android的代言。

苹果公司的iOS手机操作系统是世界上第二个智能化（第一个是诺基亚的Symbian操作系统）的手机操作平台，但是因为这个系统要依赖强大的硬件支持，同时售价昂贵，让很多人望而却步。倒是Android既无版权限制，也不会挑挑拣拣地对硬件不兼容，加上开放源代码，很多软件设计者都可以在此基础上丰富Android的系统应用，从而使得平民化的Android与贵族般的苹果系统分庭抗礼。2012年年末的统计数据表明，Android的

市场保有量已超过炙手可热的苹果，成为世界第一大品牌的智能手机平台。

“促使我不断前进的动力是通过这套平易近人的系统，我们可以天涯若比邻。我的目的是用一块数字化海绵，把全世界的人联系在一起。”

❺ 机器人情结

最爱的还是机器人，只不过这一次是把机器人合成在手机上呈现给全世界的一个玩具。安迪的机器人情结从未消失过，Android的名字来自机器人，软件的启动界面是机器人，整个智能手机从里到外都透着安迪的机器人情结。

当然，在他的家里也随处可见机器人的影子。如果家里的门铃响了十五秒仍然没有人接听，客厅门口会有一只机械手抓起一根棒球棍，敲向一面很大的锣。如果这不够高科技，那么带视网膜扫描仪的门锁就绝对可以算是“科技是第一生产力”的证明，安迪不必随身带有钥匙，想开自己家的门，只需要把眼睛凑到门上就可以。楼顶的平台上还停着几部直升机模型，只要他通过视网膜扫描就会自动起飞，来到大门口迎接主人；休息了一天的机器人们也纷纷行动，浴缸里放好热水，面包机也开始工作。甚至如果晚上不知道吃点什么好，安迪也可以按几个按钮，让那些在院子里四处游走的机器人到邻居家打探一番。

安迪以前在苹果公司的同事扎科·德拉加尼克说，“它代表了鲁宾的一贯风格：做这些只是为了享受过程，因为这很酷。所有这一切，蕴含着一股儿童般的天真。”

【黑客知识】

卡尔·蔡司公司：是一家制造光学系统、工业测量仪器和医疗设备的德国企业。由卡尔·蔡司等三位先驱于1846年在德国耶拿（Jena）建立。曾经是世界闻名的高精度照相机镜头的代名词和最大的相机制造公司。昂贵和高质量是其最大卖点，该公司生产的光学镜头时至今日仍被认为是一流的设计。

Sidekick：这是世界上第一个被应用到手机领域的基于Linux系统的智能手机平台。将无线调制解调器和模拟转换器加入带有中央处理器的手机中，使用者可以通过内置的软件在手机上连接互联网，进行简单的邮件接收和浏览网站的操作。

2002年年初谷歌创始人拉里·佩奇和谢尔盖·布林任命安迪为智能手机研发中心主任，着手进一步开发Sidekick，在随后上市的成品中，因手机功能与网络提供商的频宽问题而搁浅。

但是Sidekick系统本身是成功的和可行的，并在随后的安卓系统上得到了极好的发挥和应用。

——— 第四章 ———

E时代的X档案——阿桑奇和他的维基解密

世界上最危险的人就是那些坐在办公室里就可以掌控战争的人，人们应阻止他们，如果这样令他们视我为威胁，那也无所谓。

——阿桑奇

“这是个壮举，整个西方世界都可以松一口气了。”

阿富汗的十二月正值隆冬，户外温度已接近零度，而在国家军事防务基地的四十米地下掩体里，空调机不间歇地吹出清新逸人的空气，温度、湿度都恰到好处，四季如春。

刚刚到访的美国国防部长罗伯特·盖茨把略显肥硕的身躯塞到沙发深处，整个身心从一直纠缠着的紧张中逐渐放松开来，他微仰着头轻轻地叹了口气。“至少对我来说，这是2010年结束之前我听到的最好消息了。”

盖茨缓缓地晃动着手上的咖啡杯，杯子里香气四溢，不断旋转着的液面随着盖茨不断晃动的手生成一个小小的旋涡，像极了一张微笑的脸。

盖茨的桌上丢着一张当天的英文报纸，头版头条他已经一字不落地看了至少四遍，《强奸案告破，阿桑奇落网，外交911宣告中止》。

1 红色通缉令

能让一向以硬朗著称的罗伯特·盖茨感觉放松的事件一定是个大事件，能让一国防部长在意的人物也一定是个大人物。

刚刚过去的2010年绝对可以称作是“阿桑奇年”。这个不满40岁的流浪汉，新闻界的007，只凭一台电脑便搅得整个西方世界人心惶惶，扯动着全世界的目光紧紧跟随；他的离奇被捕，让“西方震荡”告一段落。在民众眼里，他是个新英雄，而对于西方政界和军界，他却又是个不折不扣的威胁者。他一手创办的维基解密网揭露了人类历史上披着正义外衣的最龌龊的勾当，害得中情局、FBI、欧洲军事阵线联盟的特工疲于奔命，像追捕拉登一样四处撒网，而小小的维基解密网和他的主人阿桑奇也由此成为了互联网上搜索率最高的热词之一。

2010年11月18日，瑞士当局发出红色通缉令，以强奸和性骚扰罪名通缉维基解密网的创始人朱利安·阿桑奇，原因是阿桑奇涉嫌对两名瑞典女子实施性侵犯。据这两名女子讲述，原本自愿与阿桑奇发生性关系，后因提醒阿桑奇所用安全套已经破裂并要求他重新更换，遭到阿桑奇的拒绝而被其强奸。

而在此之前，阿桑奇已经改头换面躲避数月。他染了头发，使用化名，不使用信用卡，并为自己配备了加密手机，他原来的朋友每天醒来的第一件事就是互相询问“你知道朱利安在哪儿吗”，得到的回答都是摇头。

次月7日上午9点30分，神秘莫测的阿桑奇现身伦敦一家警署，随后被正式拘捕。

当天中午，阿桑奇在伦敦威斯敏斯特区治安法庭出席听证会。瑞典检察部门指控其犯有强奸罪，法官霍华德·里德尔拒绝了阿桑奇的保释申请，而后者则拒绝了法官的引渡提议并否认自己犯有强奸罪。阿桑奇当庭

提出了自己的置疑，奇怪的是这份置疑并未涉及所谓的强奸罪名：

“我只不过是违反了游戏规则而失去了规则保护的可怜牺牲品而已，仅凭强奸罪名根本上不了红色通缉令，你们不过是想让我闭嘴而已。罪名是强奸，发出拘捕令的是瑞典，执行逮捕的却是英国，你们不觉得这很可笑吗？”

❷ 跨国颠覆

阿桑奇从他出生的那一刻起，就注定了其动荡而传奇的一生。

未满周岁，阿桑奇就死了父亲，母亲嫁给了一个三流的导演，但这段婚姻仅维持了七年，他的母亲后来又嫁给了一个毫无名气的音乐家，这个身为音乐家的继父却一门心思想把阿桑奇作为祭品献给教主——他是个忠实的邪教徒。母亲为了保住他的小命不得不离家出走，在14岁前，阿桑奇已经搬了37次家。频繁的迁徙让阿桑奇无法得到完整而系统的教育，但他却对知识充满了好奇和欲望。在搬到澳大利亚一家电子商店对面后，阿桑奇决定长居于此，因为他与这家店的老板混得很熟，并得到了免费使用店里计算机的优待，条件是他必须每天无偿给该店做4小时的义工。

就是在这台黑白显示器的破旧电脑上，阿桑奇发现了一个令他如醉如痴的新世界。每天除了打工，他就一声不响地埋头摆弄那台电脑，并在两个月后第一次编写了自己的首款软件。为了不让他每天在店里迎来送往暴露母子的行踪，母亲把这台电脑买下来作为礼物送给了阿桑奇，并给他添了一台调制解调器。可以畅游网络的阿桑奇从此以“门达克斯”[①]的名字进入网络世界，运用他完全出于自学的电脑知识周游网络，被称作“能够闯入最安全网络的高级程序员”。在接触网络后不久，他就独立编写出一

① Mendax 取自古罗马诗人贺拉斯的名言“splendide mendax”，意为“高贵的虚伪”。

个通信端口扫描程序Strobe，并将其源代码发布到网上供其他程序员完善和修改，而很多人在研究了他的程序后发现，这个程序的源代码居然没有办法再缩小哪怕一行，如此严谨、缜密的程序出自一个完全自学成才的不足20岁的年轻人之手，简直是不可思议的事情。更令人称奇的是，1997年阿桑奇与人合作，共同开发了一款主要针对人权保护和敏感信息保密工作的密码合成系统——Rubberhose Deniabl加密系统，被称作业界最完善的密码保护装置。

此后，名声在外的阿桑奇与两个志同道合的黑客朋友建立了一个名为“跨国颠覆”（International Subversives）的黑客小组，经常游走于那些号称最保险的计算机系统。欧洲经济圈——西欧联盟的网站刚刚完成了网上交易系统，并在报上称自己是“最方便快捷，最安全无忧”的第二天，阿桑奇的黑客小组便一举将其攻破。无孔不入的高深技术和天不怕地不怕的勇气，让“跨国颠覆”小组成为互联网初期最有名的黑客组织，自然也招致警方的关注。警方对这样一个猖獗的团伙，专门成立了代号“天气行动”的小组来对付他们，但这些自负的年轻人毫不在意。在调查人员第一次敲开了阿桑奇的家门做询问笔录之后，阿桑奇的母亲不得不收拾行囊，领着儿子再次开始逃亡。

18岁时，阿桑奇的女友为他生下了一个男孩。据说他的女友在耳濡目染之下也是个圈内小有名气的女黑客，曾经成功地侵入了西伯利亚石油矿物公司下属的数个计算机终端，而目的只不过是想计算一下石油生意的利润到底有多大。做了父亲的阿桑奇仍然是一名不折不扣的黑客，一边费尽心力躲避警方“天气行动”小组的追捕，一边成功闯入加拿大北电网络设在墨尔本的主终端站，并搞到了不少他的雇主感兴趣的东西。对于阿桑奇而言，做黑客真是太刺激了，“我让那些警察做梦都在喊我的名字，而那些黑客朋友都高呼阿桑奇万岁，这太美妙了。”

一天深夜，在北电网络的服务器里，阿桑奇发现系统管理员在线，得意扬扬的阿桑奇于是突发奇想，在管理员的信箱里留下了一封简短的信

件，信中极其礼貌地告之自己的到访，并声称自己发现了系统“至少四个可以被利用的漏洞，我想我可以帮得到你”，然后留下了自己租住房间的电话。

这个电话号码成为抓住阿桑奇的唯一线索。“天气行动”小组调查人员立即与电信部门取得联系，利用技术手段24小时侦听这个电话，并要求北电网络的系统管理员给阿桑奇回信，声称自己想拜阿桑奇为师学习黑客技术。在掌握了大量证据之后，1991年10月29日，警务人员敲开了阿桑奇的家门。

阿桑奇被指犯有非法入侵国家公共网络，及商业间谍等共计31项罪名，最高可判处十年监禁，但阿桑奇要感谢他的辩护律师。在律师的据理力争之下，最后法庭只是以“除了有些智力上的好奇心和能够在各种电脑上冲浪的愉悦之外，没有证据表明还有什么其他问题”，判阿桑奇缴纳为数不多的一小笔罚金便不了了之，被当地警察称为“史上最可笑的宣判”。因为从阿桑奇被捕到宣判结束只花费了不足一个月的时间，而数十名高科技警员仅仅为了抓捕阿桑奇及搜集证据就花费了3年时间。

❸ 网络世界的罗宾汉

在此次被捕之前，自学成才的黑客阿桑奇为了躲避警察，带着母亲和女友以及他的孩子几乎走遍了澳大利亚的所有城市。从小到大，他上过三十七所学校，其中包括六所大学。颠沛流离的生活造就了阿桑奇坚韧果敢的性格，对待任何事情都保持冷静的头脑和不苟言笑的冷峻表情，包括女友带走自己的孩子。

女友实在无法忍受这种居无定所的生活，在阿桑奇入狱期间不辞而别。重获自由的阿桑奇于是开始寻求法律帮助要回孩子，在历时三年后终于重新得到了孩子的抚养权。在这之后，他同时打六份工养活母亲和自己

的孩子，并把一头黑发染成银色。多年的半隐居生活、法院受审及女友出走等这一切，让阿桑奇开始痛恨权威，痛恨那些衣冠楚楚却言行不一的虚伪。

这种仇视当权者的性格，促使阿桑奇必须要体现自己的正义来拯救世界（这一理想化的生存目的几乎是所有黑客的心理特征之一）。阿桑奇认为政府和大机构隐藏了太多的秘密，而这些秘密只被政权内部极少数人所知，这就形成了一个神秘的沟通线路。这个线路一旦被破坏，阴谋家们的信息交流就会缩小，当这种沟通趋于零的时候，真相就将大白于天下，阴谋就会不攻自破。而使这些信息昭于天下的任务，不妨就交给他自己来做，“我的工作是为了自由而奋斗。”

黑客一旦结合成团体，其活动范围和能量都是巨大的，他们可以得到网络世界上最机密的文件，并以他们认为值得的可靠方式进行传播或保存，这些机密成为他们与当局讨价还价的资本，或是直接将其转变为钞票。而阿桑奇的目的不在于金钱，“如果只想得到金钱，我只需要做一名最优秀的黑客就够了。我的理想是改变我所生活的这个国度，以正义之名维护真相。”

2006年，阿桑奇把自己反锁在乡下一间出租房里，开始构建他的理想国。他从源代码阶段开始编写一个网站系统，不采用大公司的现成网站合成软件的原因在于，他并不相信那些网站合成器的可靠性和稳定性，“我只相信我自己，并且我有能力可以展现只有我才具备的个性特征而其他人无法模仿。”这个被命名为“维基解密”的网站被架设在一家名为PRQse的网络空间服务器上，阿桑奇把自己认为有价值的信息通过特殊的网络中转形式，保存于设在比利时的另一台服务器上，而在这个传输过程中，阿桑奇自信地采用了自己研制的Rubberhose Deniable加密系统。

当年12月，维基解密公开了它的第一份机密文件：阿桑奇的伙伴们从来往于某个敏感网络的数以百万计的加密文件中，成功分离由索马里反政府武装“伊斯兰阵线联盟”领导人谢赫·哈桑签署的秘密决定。

这一决定的成功解密，让美国人也大吃一惊。这决定中的内容，美国人也曾梦寐以求而不可得，却被一个民间网站成功破译，这不能不说是个奇迹。

维基解密有关这份决定的解密和公开，远远超过了文件内容本身。维基解密也第一次被世人重视，甚至荣登美国“最值得关注的危险来源地址”之一，因为高度发达的美国互联网中，每天都流动着庞大的绝密信息，而这些信息是最不能为人所知的。维基解密的存在，让美国人既感到欣喜若狂又深感恐慌，因为维基解密的出现让美国人得到了很多高级间谍也拿不到的情报，又时时感觉到自己的信息保密工作在那些黑客眼里，是如此的不堪一击，哪怕是一次泄密，对美国人而言都可能是灭顶之灾。

4 外交史上的“9·11”

美国式的聪明就在于，很多事情不管它是不是美国人希望看到的，总是能被山姆大叔不幸言中。不久之后，在美国人窃喜可以每天从维基解密网站上得到珍贵的情报之余，他们自己也成了维基解密的攻击对象，从肯尼亚政府的腐败内幕到关塔那摩监狱的虐囚事件都让美国人坐立不安。2010年4月，一份美国对伊作战的录像曝光，录像中美军的阿帕奇武装直升机向平民疯狂扫射并造成多人伤亡；7月，维基解密公布了7700万份美军在阿富汗战争期间的绝密战争数据资料；10月，维基解密又一次抛出重磅炸弹，公布了一份美军在对伊作战期间对平民的屠杀和非法用刑。由维基解密公布的伊战美军死亡人数与美国先前公布的数字相去甚远，这个被美国政府严重压缩了的死亡人数，一向被认为是美军对伊作战“完胜”的最有力证明，一旦证实维基解密公布的数字具有真实性，美国将颜面扫地、威风不再。

这让一向自认高人一等的美国人如坐针毡。

冷战结束之后，塞尔维亚总统米洛舍维奇、波黑总统卡拉季奇、伊拉克总统萨达姆……众多美国全球战略统一思维体系中的障碍被一一清除，美国正处于春风得意、高歌猛进之时，突然杀出的维基解密让美国人措手不及。令美国“很受伤”的对手阿桑奇及他的维基解密，手中掌握的并不是飞机大炮，而只是一台电脑和一根网线就足以让一个超级大国倍感恐慌。

在国民对政府的信任度一再下滑的时刻，维基解密不断把美国政府的短处拿出来，让这个霸主级国家丢失颜面。克林顿声称自己与莱温斯基清清白白；小布什大力宣扬萨达姆拥有大规模杀伤性武器；奥巴马说阿富汗战争胜利在望，对伊局势指日可待，一再声明不参与韩朝争端等言论……领导人的高谈阔论与维基解密展示给众人的现实真相相去甚远，这一切都让普通民众对美国政府大失所望。维基解密在给美国政府雪上加霜的同时，几乎得到了全世界的拥戴。

2010年11月29日，中国最大的综合网站“新浪”网报道，维基解密将超过25万份美国驻全球各地的使、领馆或代办处发给华盛顿的电子文件内容在网上曝光，时间从2004年以后直到“昨天”，这些文件的内容措词极为“坦率”，让美国遭遇了建国以来最大的尴尬，其中很多戏剧性的情节让这个急欲在全球范围内谋求霸权的国家极为难堪。美国在这些文件中把伊朗总统内贾德称为“第二个希特勒”，称德国总理默克尔是“特富龙天使”，俄罗斯总统普京“是男人里最透明的”，俄罗斯总理梅德韦杰夫则“随时充满担忧和犹豫”，还把“赤裸君主”的头衔大度地赐予了法国总统萨科齐，而奥巴马自己则“更喜欢东方而不是西方，对欧洲完全没有感情和归属感”。

所有西方国家的领导人都密切关注维基解密，意大利外长法拉提尼对以上资料的曝光“深感遗憾”，将这一事件形象地称作“全球外交史上的‘9·11’事件”，并声称若任其发展而不采取强硬措施，将由此引发一场世界性的外交大灾难。

❺ “有罪的人才会痛”

阿桑奇的被捕是意料之中的事情。

2010年11月，针对阿桑奇的红色通缉令正式由国际刑警组织下发，而阿桑奇则仅携带一台笔记本电脑和一个背包，悄无声息地隐入人群。

从小过着吉普赛人生活的阿桑奇习惯了流浪，警惕而坚忍的性格也让他从未想到过屈服，但面对整个西方世界经验老到的刑警组织，阿桑奇仅凭一己之力根本无法与之抗衡。在逃亡途中，阿桑奇致信媒体，声称自己和他所运行的维基解密仍掌握着数十万份相关资料，“足以让美国和他的附属国摔一个大跟头。”并以此为筹码要求国际刑警组织取消红色通缉，“归还属于我的自由和安全。”

但是阿桑奇还是在“被FBI贴身跟踪了四天之久”后，不得不在英国伦敦以自首的方式结束逃亡。在警局里，他先是自报家门，然后要了杯水和几片面包，接着就躺在椅子上睡了过去。三小时后，阿桑奇睁开眼的第一件事，就是又要了一杯水和几片面包，然后要求找一个剃须刀来，以便“我出现在报纸或电视上时，人们应该看到一个精神饱满的朱利安”。

以强奸罪遭到通缉的阿桑奇，自始至终对自己的罪名感到莫名其妙。“那两个女人本来是自愿与我发生性关系的，只不过后来在安全套的问题上出了点小摩擦。就像不能因为我使用了一只坏掉的安全套就告我强奸一样，你们也同样不能用强奸罪来让维基解密闭嘴。”

而他的律师则用一句话点醒了他，“你在规则之外行事，他们自然就得要在规则之外对付你。你违反了游戏规则，自然也就不受规则保护。”

对此，阿桑奇只能付之一笑。

在阿桑奇被捕之后，近60万名维基解密的支持者联名呼吁支持阿桑奇，口号是“尊重信息自由公开，新闻自由公信，法律自由公正”。维基解密的拥护者声称，新闻现在已经演变成一种被阉割的政治宣传机器而不

是揭开真相的工具，他们宁可相信维基解密的数据和信息是正确的，但显然法庭不会被网络呼声所左右。

美国政府新闻发言人克劳力说，美国官方一贯认真对待机密信息的流通环节，而以黑客手段截获和破解相关信息是违反美国法律的，它将威胁到美国国家安全并扰乱民心，打击政府在民众心目中的良好形象，而且这些信息缺乏应该具备的可信度，因为其来源渠道非正规也非法，虽然影响巨大，但不应该被明智和理性的民众所接受，并声称阿桑奇是个打着自由和真相幌子的超级骗子。

这番纯属外交辞令的话多少显得苍白无力，阿桑奇的律师则反驳说，如果这些数据和信息纯属子虚乌有，就不会有那么多惊弓之鸟，阿桑奇也不会遭遇跟踪、逮捕和暗杀威胁，并在法庭上将阿桑奇和他的维基解密比作“信息时代的詹姆斯·邦德”，是追求真相的刀锋战士，维基解密应该受到保护而不是打击。

一直与阿桑奇相依为命的母亲克里丝汀·阿桑奇在事发之后也赶到伦敦，在一次对话中，她不无担忧地问自己的儿子这样做是否值得。阿桑奇回答：“我的信念坚定不移，我仍然忠于我的理想，不会因自身的遭遇而改变信仰。无论发生任何事，都只会更坚定地相信，我的理想是真实而正确的。”

阿桑奇虽然被捕，但维基解密仍在运转，这个神秘的机构共有九名董事，只有阿桑奇一人的身份是公开的，其他八人仍是阿桑奇的忠实战友。维基解密没有固定的办公场所和总部地址，只是在伦敦某处的地下室雇了几个打字员而已，遍布全球的八百余名志愿者才是这个机构最坚实的力量源泉。维基解密的发言人声称，如果阿桑奇的引渡计划失败或被判有罪，“那么全世界都将再次陷入动荡和混乱”，但显然这一次以美国为首的维基解密受害者们不想放虎归山。

法庭至今仍未对阿桑奇量刑，法庭的借口是取证困难，而阿桑奇则兴奋地宣称这是一个民间网站对整个西方世界的胜利，“不敢断定有罪，正

说明了某些人内心里充满焦虑和恐慌，而这更让我对自己所做的事业感到无上的光荣。”

早在被捕之前，11月11日，阿桑奇接受了《福布斯》的记者专访，在访问中，阿桑奇声称维基解密创立了一种全新的新闻理念，而这个理念的中心词只有两个字：真实。

真实是新闻的基础，在普遍意义上，新闻的接受者无法确定他们所看到新闻的真实性有多少，然而维基解密则在其中起着不可替代的对新闻或史实真实性的验证功能。“科学的新闻理念允许读者阅读一篇新闻，然后点击鼠标，在网上找到产生新闻的原始文件。这样，读者就能够自行判断：这篇新闻是否真实？记者的报道是否准确？民主社会需要强势的媒体，而维基解密正是这种媒体的一部分。媒体可以使政府不敢否认自己的错误并由此变得更加诚实。而任何国家和权力机构，都无权枪毙一个说真话的人。”

对于揭露丑恶是否感觉很痛快这一问题，阿桑奇毫不掩饰自己的兴奋，“这能给我带来满足感，亲眼看到改革的兴起，知道自己在这个过程中曾发挥了怎样的作用，看到社会的良性发展，新鲜的血液在滋生，而滥用权力者和蒙蔽大众视听的人得到应有的惩罚，民众看得到真实的一面，并美满的生活着。这就够了。”

“可是揭露社会丑闻会让很多人感到痛苦。”

“有罪的人才会痛苦。”

【黑客知识】

维基解密：这是一个专为揭露政府、企业腐败行为而成立的网站，成立于2006年。因其多年来一直处于幕后并不断地爆出猛料，让众多西方国家抓狂，随着美军暴行的连续披露，这个以朱利安·阿桑奇为首的神秘组织极速蹿红，成为目前最炙手可热的网络关键词。

该网站没有对外界公布办公地点和电话，不公布主要运营者的姓名和网站所有人的入网信息，没有人知道其总部的具体位置、运营模式及人员分配情况，这甚至不是一家注册公司。目前所知道的情况是，它依靠着一支遍布世界的志愿者来维系其基本运营，运营资金仍来自志愿者的捐助以及团队成员自掏腰包，其职责为专门公布机密“内部”文件，宣称要揭发政府或企业的腐败等不法内幕，追求信息透明化。

维基解密解了哪些密？英国《每日电讯报》2010年7月26日梳理了“维基揭秘”近几年来所泄露的几大“不能说的秘密”。

A. 美军袭击伊拉克平民视频

在“维基揭秘”网页上有一段视频录像显示，驻伊拉克美军士兵在直升机上朝地面的人群开火，结果造成包括2名英国路透社记者在内的18人死亡。

B. 关塔那摩监狱手册

2007年，“维基揭秘”公布了一份美国国防部下发给士兵的《关塔那摩监狱管理指导手册》。该手册内容显示，监狱管理士兵有权阻止红十字会工作人员探视囚犯。如果被关押人员表现良好或是积极与军方配合，还可获得“特别奖励”，而这“特别奖励”就是一卷手纸。

C. 气候学家擅自更改数据

超过1000封英格兰东安格利亚大学气候研究所的邮件内容被公布在“维基揭秘”网站上。邮件内容显示气候学家擅自更改对自己研究不利的气候数据，以证明全球气候变暖主要是由人类活动造成的。此事导致人们对全球变暖理论产生怀疑，影响很恶劣，外界纷纷指责科学家操纵研究结果的行为。

D. 佩林私人邮件

在2008年美国总统竞选期间，美国共和党总统候选人麦凯恩的竞选搭档佩林的私人邮件账户曾被黑客窃取，之后她和家人的大量私人照片以及一些邮件内容被“维基揭秘”网站公布在网上，引发民众热议。

E. 50万条“9·11”短信

2009年11月，“维基揭秘”网站曝光了超过50万条“9·11”恐怖袭击事

件发生当天美国民众通过手机发送的短消息内容，其中包括美国联邦政府以及地方官员的短信。“维基揭秘”表示，这批短信是匿名人士提供的，他们公布这些短信只是为了尽可能地还原“9 · 11”恐怖袭击事件发生当天的情形。

国际刑警红色通缉令：这是国际刑警组织间频繁使用的最著名的一种联合通告，它的通缉对象是有关国家的法律部门已经判决有罪而仍然在逃、能够造成极重大社会危害，且极度危险的罪犯。这个通告是在世界范围内一经确认即可逮捕并有权临时扣留的国际证书，无论哪个成员国接到红色通缉令，都应立即布置在本国范围内对嫌犯的通力搜寻，如发现下落，应迅速组织警力实施抓捕，并将其缉拿归案。

——第五章——

马克·扎克伯格，Facebook的黑客国王

当你拥有五亿个朋友时，怎么能不树几个敌人呢？

——电影《社交网络》的导演大卫·芬奇[①]

原微软中国总公司经理吴士宏说过：“无论什么理想都要先生存。”这句话算得上是个朴素的真理。小时候的作文里，有关《我的理想》一类的文章里总是把科学家、老师、军人这类不一定伟大但至少可以说算得上高尚的职业拿出来说事。但对于普通人来说，先求温饱，解决不了温饱，一切都免谈，精神饱满一定是要建立在肚子饱满之上。在温饱的基础上，似乎所有人都做过一夜暴富的梦，但实现起来，有相当的难度。从床上爬起来，穿衣吃饭，继续挤咱的公交车去。

而一旦有了点石成金的机会，相信每一个人都不会轻易放过，尤其是那些善于把握机会的人。

① 大卫·芬奇（David Leo Fincher），1962年8月28日出生，美国科罗拉多州丹佛市人。美国著名电影导演及MTV导演，主要代表作品有《社交网络》、《七宗罪》、《搏击俱乐部》、《本杰明·巴顿奇事》、《龙纹身的女孩》等。

1 Facebook效应

所谓童话，通俗来说无非两套情节，一是灰姑娘终于穿上了水晶鞋，二是癞蛤蟆吃到了天鹅肉。马克·扎克伯格虽然不是癞蛤蟆，但他无疑吃到了天鹅肉。仅从那件汗衫和随意趿在脚上的旅游鞋，以及满脸的稚气，你无法相信就是这个看似乳臭未干的小子，一手创建了世界“第三大国”。也就是这个名叫扎克伯格的小伙子，击败了苹果公司CEO乔布斯和风头正劲的阿桑奇，成为2010年度《时代》周刊的封面人物，也是《时代》周刊自1927年以来最年轻的封面人物。《时代》周刊的总编辑理查德·斯坦格尔说：“扎克伯格的入选是因为他完成了一项前无古人的伟大壮举：把世界上十分之一的人口联系在一起，并由此建立起一个和谐美好的进入良性运转状态的社交关系。”

这个虚拟世界的“第三大国”，人数仅次于中国和印度，它有一个很戏剧化的名字：Facebook（脸谱）。

应该说，扎克伯格也是个淘气小子，曾扮演过一两次黑客，但他玩黑客纯粹是个性的展现，按他自己的话说，从不把自己的快乐建立在别人的痛苦之上。从幼年起，扎克伯格就表现出异于常人的电脑天赋，他6岁时就开始独立编程，12岁的时候把学校的主页搞成自己的相册，并自称天下第一帅。甚至到了大学（忘了说一句，他和计算机界的大哥大比尔·盖茨一样，读哈佛大学），再一次把学校的主页用自己的照片替换掉，并在主页上发起了一次“帅与不帅”的投票。甚至在一夜成名之后仍然不改天真顽皮的做派。在Facebook成功之后，比尔·盖茨执掌帅印的微软公司也向他伸出了橄榄枝，并邀请他“见面谈谈”。要知道无论是谁，能接受微软高层领导人的会见都是相当难得的机会，世界上多少知名的企业家求之不得，而这个20岁刚出头的小伙子居然一口回绝了，理由你绝对想不到，因为微软要求的见面时间太早了，而“我有睡懒觉的习惯”。

就是这样一个特立独行的毛头小子，在短短的四年时间里，把一个学校级的主页空间经营成世界排名第八的知名网站，而它的主人也因此告别哈佛这所世界级的名校，由一个不太光彩的辍学生一跃成为路人皆知的互联网领袖。

❷ 把哈佛丢在脑后

扎克伯格和他做牙医的父亲一起生活在纽约市北威郡的郊区。父亲的生意一直不错，络绎不绝的病人让诊所的护士很是头疼，于是12岁的扎克伯格用了一周时间编写了一个病人接待程序，通过这个程序甚至可以在家里与诊所互动，即时了解诊所的情况，这个程序后来被周边的孩子们热烈追捧，成为“可以躲在家里和朋友聊天的好玩意”。而扎克伯格也由此在小镇上声名鹊起，成为众多女孩子心中的白马王子。

以扎克伯格的性格，他永远不会是个乖孩子，却也绝不会是个只会读书的呆子。事实上他活泼好动、快人快语。在哈佛，他是学校击剑队队长，还拿到了文学学士学位，甚至写过几本不错的书，当然，那时候还没有出版社垂青这个一文不名的小子。他更多的时候是把自己反锁在房间里编程序。他开发的程序简洁易懂又有极高的技术含量，甚至AOL和微软公司都对他的程序感兴趣，很想拉拢他成为自己的一员；但一向喜欢无拘无束生活的他，很难把自己固定在某一个行政制度健全而严格的团体里磨灭才华。高中的时候，喜欢一边编程序一边听音乐的扎克伯格，用了两杯咖啡的时间编写了一个播放器。这个名为Synapse的播放器，可以按照收听者的喜好，自动把收听率最高的曲目排在最前边。微软公司当时甚至想用200万美元收购这个播放器，耍酷的扎克伯格却一口回绝了，随后他把这款播放器作为自由软件放到了互联网上任由喜爱者免费下载使用。后来一对双胞胎兄弟邀请他合作完成一个社交网站，仅仅两个月之后，他又撒手

不干了。这一回他突发奇想，自己搞了一个思路新颖的社交网站，这就是Facebook的雏形。

就在这期间，他在某个午夜百无聊赖地侵入了学校的主页，并在上面放上了两张自己的照片，然后让浏览者投票“哪一张更帅一点”。

学校的主页当然很快就被修复了，扎克伯格也自然被狠批了一顿。学校的条条框框和故作斯文显然并不适合他的性格特点，而更重要的一点是，他刚刚建成的Facebook长势喜人，在短短时间里便很受年轻人欢迎，注册人数节节攀升。于是，被戴上“捣蛋鬼黑客”头衔的扎克伯格索性离开了一本正经的哈佛大学，成为一名逃兵回到家里，一心一意地研究自己的Facebook去了。

❸ 把钞票放在兜里

令人奇怪的是，这个喜欢玩酷的小伙子虽然拒绝了200万美元，却接受了一份1000美元的资助。一个名叫爱德华都·萨瓦林（Eduardo Saverin）的年轻人，替Facebook租下了一个相对稳定的网络服务器。对于萨瓦林与这似乎微不足道的1000美元，一个朋友的解释是“萨瓦林觉得他可以从这个网站上挣到钱”，而扎克伯格的回答很干脆：“他有着良好的社会背景和运营经验，他也会帮我们挣钱。”

互利互惠成为二人合作的最基本因素。于是，这两个年龄加起来尚不足50岁的年轻人对视一笑，一拍即合。

扎克伯格于2004年1月12日以每月85美元的价格在纽约租用了服务器，并注册了The Facebook.com的域名，因为Facebook.com这个域名被人抢注了。扎克伯格于是埋头苦干，重新设计网站的格局，并思考和定位其经营方式，萨瓦林则理所当然地以1000美元的代价占有了这个网站30%的股份并出任CEO。直到一年半以后，财大气粗的扎克伯格才花20万美元

去掉了那个看上去相当别扭的定冠词“The”。

Facebook不是世界上第一个社交网站，在它之前已经有过无数成功的先例，扎克伯格的另类在这里派上了用场。他一改其他交友类网站的建站模式，从一小撮熟悉的朋友开始，一点点扩大这个社交圈。同时特别注意保护用户的隐私，别的网站只需要点击鼠标就可以把一个陌生人加为好友，而在Facebook上，你必须经过主人的同意才可以这样做，主人甚至可以设置自己的哪些资料可以被哪些人搜索到。这个看似不起眼的改进，让每个来到这里的人都感觉自己是安全的，不会被恶意骚扰，如此贴心的设计为Facebook赢得了大批的注册用户。在最初的几个月里，Facebook就牢牢地圈住了3000多正式注册用户。虽然3000并不是一个很大的数字，但可以试想，在哈佛这个只有5000人的学校里，居然有一大半的学生在这里流连忘返，这不能不说是一个惊人的覆盖率。由这3000个人开始，随后几何级增长的注册用户让Facebook像竹子一样疯长起来。在此之前，似乎没有一个网站的成功如此迅速过，两个月后，哈佛校长在当年的毕业答谢会上也对这个由哈佛辍学生建起的网站赞不绝口。为了应付剧增的数据，扎克伯格招入了自己在哈佛的同班同学杜斯丁·莫斯科维茨（Dustin Muskovitz）帮自己打理网站，并从自己的股份中出让给莫斯科维茨5%，但就在这之后不久，三个合伙人的关系却急剧恶化。

❹ 金钱、天才和背叛

“合久必分，分久必合”可以说是放之天下而皆准，如日中天的Facebook也逃不开这个魔鬼咒语。暑假时，除了扎克伯格之外，另外两个学业在身的合伙人都有了大把的时间自由支配，虽然仅仅埋头于网站的运营就足够他们打发这些时间，但显然扎克伯格不想囿于现状。他决定出去走走，见见世面，莫斯科维茨当然追随其后，二人商量的结果是，把这个

蒸蒸日上的网站推向加利福尼亚的高新技术密集区。那里有更好的发展空间可以让他们大展拳脚，在那里可以继续扩大团队规模，并创造某个可能的融资机会，从而将纯娱乐性的Facebook尽快转入商业运营模式，而萨瓦林则决定去纽约雷曼兄弟公司实习。

萨瓦林对二人的加利福尼亚之行并不十分热衷，理由很简单，网站虽然形势喜人，但实际上一直在掏萨瓦林的腰包，而且扎克伯格此行的预算将达到惊人的1万美元，注册人数的剧增也对服务器的流量提出了更高的要求，为了维持网站正常的数据访问，萨瓦林必须要再掏钱租用更高级别的服务器，这笔花费也不在少数。三个人的第一次争执便不可避免地开始了：扎克伯格认为加利福尼亚有着广阔的发展前景和不可限量的商业机会，而萨瓦林则认为与其花费巨资进行一场未知结局的探索，不如直接在目前看上去还不错的网站上植入广告来得稳妥和实惠。

“没有人能阻止得了扎克伯格，否则他也不会拒绝微软的200万美元，而对萨瓦林的区区1000美金感兴趣了。事实上从认识他的那一天起直到现在，他一直是个一旦认准了就要不计后果做到底的固执家伙，奇怪的是，每一次他的选择都是对的。”莫斯科维茨对他的合伙人叹为观止。

在加利福尼亚，扎克伯格每天穿行于各大网络公司之间，不停地与知名的网络人接触、交流和学习。在这里，早已扬名硅谷的音乐网站Napster负责人肖恩·帕克成为了扎克伯格的良师益友。

帕克认为：按目前Facebook的发展前景和运营思路来看，早晚有一天，这将是一个足以改变互联网事业的优势网站；在羽翼未丰之前，Facebook急需的不是用植入的广告挣那些微不足道的钞票，而是继续培养和扩大相对稳固的用户群。帕克的想法与扎克伯格不谋而合，扎克伯格毫不犹豫地又捐出了自己股份的一部分邀请帕克进驻Facebook，希望依靠在互联网中摸爬滚打了多年的帕克，用其丰厚的实践经验让还在发展中的Facebook，尽早地进入一个新的、良性的历史发展时期。

而远在纽约的萨瓦林显然对自己的公司新加盟了股东一事毫不知情，

急功近利的萨瓦林简直是有些迫不及待地在网站首页上加入了广告。并不明智的萨瓦林也许是故意和扎克伯格赌气，这个首次出现在Facebook上的广告内容，居然是萨瓦林个人拥有的一个求职网站的链接。

这让扎克伯格暴跳如雷。“你应该知道，我们的网站发展前景规划中很清楚地写到，在不久的将来，Facebook也会拥有自己的求职版块；而你居然自己悄无声息地早就经营起这个来了，并且还把这丑陋的东西链接到神圣的Facebook上来，这不仅仅是糟透了，简直就是卑鄙。”

同时在网站的融资问题上，萨瓦林显然也犯了一个很低级的错误，在网站蒸蒸日上的时候，与网站的最大股东扎克伯格意见不合。

到目前为止，网站的发展超乎所有人的想象，在短短的六个月时间里，网站的注册人数就突破百万大关。当初租用的小服务器根本无法支撑如此巨大的访问请求，这就对萨瓦林的口袋提出了更高的要求。

按说前景如此看好，萨瓦林是很乐意把钱掏出来的，问题是，莫斯科维茨与扎克伯格的加利福尼亚之行看来比预期的效果更好，很多互联网产业的大鳄也都对Facebook颇有兴趣，排着队找扎克伯格送钱，希望在未来的某一天可以在Facebook上分一杯羹。扎克伯格也显然是每天忙于会见那些巨头人物，每天在自己的简短得不能再短的电话里，喜形于色地大肆宣扬某某又有了什么新点子，只要自己点点头，就可以有多少多少美金流到公司的账户上来。而这一切，本来就应该是萨瓦林的事情。

隐约之中，萨瓦林感觉扎克伯格在有意回避他这个CEO；同时由于大量资金的融入，萨瓦林虽然小有资产，但显然无法与那些一掷千金，在互联网产业摸爬滚打了多年的人物相抗衡，他甚至感觉到自己已经摇摇欲坠了。

万般无奈之下，萨瓦林做出了一个极不明智的选择，他冻结了自己的银行账户，或者说他想通过这种手段切断Facebook的资金链。他明明知道，现在扎克伯格缺的不是钱，他只是想敲山震虎，只是想提醒扎克伯格不要继续忽视自己的存在；但这一次他又错了，扎克伯格最不喜欢的就是

坐在功劳簿上耀武扬威。

扎克伯格还是很念旧情的，毕竟在网站最初成立时，是萨瓦林站在自己身边，向这个前途未卜的事业投入了极大的财力和精力。他打电话给萨瓦林，希望他能到加利福尼亚来一次，“共同决定公司未来五年的发展。我知道你也不想眼睁睁看着它垮掉，可是让我灰心的是，组建团队、得到融资、打造商业模式这几样最重要的工作，作为CEO，你显然一样也没有漂亮的完成。你在最近的一个月里干的最漂亮的事就是在Facebook的首页上，弄了个恶心至极的广告。”

萨瓦林显然已经气急败坏，他一口回绝了扎克伯格的邀请。“谢谢你给我买的头等舱机票。不过我想，我们敬爱的股东先生完全可以把这张机票交给哪个漂亮的金发女子，让她飞过去安慰一下你疲惫的身体。”

本来扎克伯格还在一直犹豫要不要再扩大融资范围，萨瓦林的举动彻底打消了他的顾虑。就在萨瓦林建议他找个“漂亮的金发女子”的第二天，扎克伯格敲定了共计75万美元的首次融资，同时坚定了他的“断腕”念头：当务之急就是清理门户，把萨瓦林扫地出门。

❺ 黑客CEO

到目前为止，虽然扎克伯格进行了大量的融资，但并没有继续把公司的股份分割出去，三大股东分别是自己占全部股份的65%，萨瓦林占30%，莫斯科维茨占5%。每一个股东都不会在公司处于快速壮大的时候主动退出的，甚至都无法赶走，但扎克伯格早已在萨瓦林身上磨尽了耐心，他再也不想让这条腥鱼搅了这碗好汤。“也许这个时候把萨瓦林驱逐出去，没什么实质性的好处，但就像一艘快速前进的船，我不想在顺风的状态下遭遇一场横风，我需要控制权。”

扎克伯格的态度很坚决。2004年7月末，Facebook被重组，吸收帕克

等融资人成为新的股东，当年10月的最后一天，扎克伯格诱使萨瓦林签署了股东协议，在这份协议里，扎克伯格将自己股份中的一部分分给帕克等融资人，使自己的股份由原来的65%降为51%，而将萨瓦林的股份由原来的30%提高到35%，作为交换，萨瓦林同意将原公司的知识产权中属于萨瓦林的那部分全部移交给新公司，也就是说，在网站的知识专利上，萨瓦林再没有任何技术股份和参与权。同时，萨瓦林在协议中同意在自己不在场的情况下，由扎克伯格代为行使自己在公司的投票权。

在众多的金融大师的帮助下，扎克伯格这招偷梁换柱取得了巨大成功。萨瓦林是个精明的人，但却天真地忽视了一个最重要的东西：扎克伯格所持有的股份是具有结构防稀释功能和转移权的优先股，而自己的这35%股份只是普通股，虽然净资产一下子涨到了几百万美元，但动荡的股市会泡沫一样席卷一切。

签署完这份协议之后，萨瓦林便美滋滋地回到学校继续他优哉游哉的学习了。而扎克伯格则紧锣密鼓地继续着他的“稀释计划”：2005年1月，扎克伯格先后两次通过了大量发行普通股的决议，并由自己代萨瓦林投了赞同票，萨瓦林的股份被迅速地稀释到10%以下；3月28日，公司新股再次上市，萨瓦林的股份瞬间变为0.05%，几乎可以忽略不计。蒙在鼓里的萨瓦林此刻还在哈佛的教室里举手回答问题。直到当年的4月，萨瓦林这个Facebook名正言顺的CEO在签署有关公司第二次融资的文件时才发现，自己在Facebook除了拥有CEO这三个英文字母之外，几乎一无所有。

15天后，扎克伯格在自己的办公室里接见了萨瓦林的律师，并在随后的公堂对簿中大度地给萨瓦林7%的公司股份，但要求萨瓦林以当日收盘时的股票价格将股份变现，不允许他持有这些股票。

萨瓦林的1万美金投资，在不到两年的时间里，戏剧性地增长超过了1000万美元，这是唯一能让萨瓦林感到欣慰的一件事情了。

Facebook在短短数年的时间里风靡全球，就连美国总统奥巴马、英国女王伊丽莎白二世也成为其中一员，其市值保守估计超过1800亿美元。扎

克伯格也在其中如鱼得水，从一个辍学生一跃成为世界上最年轻的亿万富翁，与他的校友比尔·盖茨一样，他们都是“学习不好的坏学生”，但都是白手起家，成就了互联网的伟大传奇。

值得一提的是，扎克伯格无论在多么正式的场合下都从不穿西装，甚至在与社会名流或是政府高官会见时，仍然穿着他在街市上买来的1.5美元一双的旧拖鞋。他每天依旧骑自行车上班，端了杯咖啡把自己丢在电脑前，和员工们一起挤便当店、一起编程序，直到现在，他仍和自己的女友住在租来的一间不足20平米的廉价房里。

简约、时尚的Facebook的背后，有一个疯长的用户群，也有一个疯长的年轻的小伙子，当然，也有不少敌人虎视眈眈，这其中就包括对他恨之入骨的萨瓦林。萨瓦林甚至为此专门出版过一本名为《偶然诞生的亿万富翁——关于性、金钱、天才和背叛》，把扎克伯格描写成一个庸俗至极的好色之徒。很好理解，就如扎克伯格的传记电影导演大卫·芬奇所说：“当你拥有五亿个朋友时，怎么能不树几个敌人呢？”

⑥ 后记：一个失恋男生的自白

我的名字叫马克·扎克伯格，我是一典型的鬈发犹太人，我成绩优秀，高中最爱编程，造了几个有点小用的软件后，我考上了哈佛。在大学我什么都不缺：社交，那是上等社会有钱小孩的游戏，我羡慕但我不需要；女朋友，有一个我无比喜欢的女生Erica，但她没我聪明，从她去波士顿大学就知道了。我不会甜言蜜语，我向来直言直语，这就是为什么我女朋友会叫我*sshole然后和我分手。我生气，我愤怒，于是我在博客里说了她的坏话，我还专门因此建立一个叫做facemash的网站来表达我对所有女生的不屑。我一小时内编程出来的网站，在两小时内因为流量过大造成哈佛的网络系统瘫痪。那又怎样？ 我什么都不怕。

两个傻呵呵的兄弟找到我，并告诉我他们想建一个哈佛学生自己的社交网站，他们叫它The Harvard Connection。我觉得这主意不错，所以自己编了另一个网站叫做The Facebook。我和我的好朋友爱德华都·萨瓦林一起合作，他出钱，我出力，我70%的股份他30%。傻呵呵兄弟不爽了，觉得我偷了他们的想法，但我觉得我没做错。好朋友爱德华都·萨瓦林也不爽了，因为我听信他人的流言蜚语，最后把他的股份降低到0.03%而已。他面对着我，并在律师面前说："马克，我是你唯一的朋友，而你背叛了我！"

我无言以对，我坚信我不是坏人，但这一切为了什么。最后我成为了全天下最年轻的亿万富翁，用仅仅几百万美元封住了这些人的嘴。但我孤单得只剩下Facebook，还有钱陪着我。

当故事结束时，我坐在我的电脑前，通过Facebook找到了那个我曾经深深喜欢的女孩子。我一遍遍看着她的头像，犹犹豫豫地加了她为好友，又一遍遍地刷新，期待着她能通过我的好友认证。但最后，我知道我其实任何等待的希望都没有了。她又怎会知道，这个价值6.4亿美元的网站只是我当时因为她离开我，而伤心难过时建造的呢?

【黑客知识】

Facebook：一个大名鼎鼎的社交网站，是美国排名第一的照片分享网站，中文音译为"非试不可、非死不可"，意译为"脸谱"，2004年2月4日正式挂牌上线。从2006年9月到2007年9月的短短一年时间里，该网站在全美网站中的排名由第60名上升至第7名。据2010年的统计数据表明，Facebook每月有5700亿页面浏览量，站内照片存有量比其他所有图片网站加起来的还要多，每个月超过30亿张照片被上传，Facebook的系统每秒要处理120万张照片。如此巨额的数据处理需求，使得Facebook目前有超过30000台服务器为其服务。谷歌是目前

美国最大的网站，覆盖了81%的美国人口，Facebook落后于谷歌、雅虎和微软排名第四，其数据服务覆盖了53%的美国人口。这是世界互联网历史上的一个奇迹。

Facebook的近期发展目标为继雅虎之后，成为世界上另一个有着良好背景的互联网搜索引擎。

世界上最著名的辍学生：

A. 比尔·盖茨

比尔·盖茨的幸运数字是1和3。他13岁开始疯狂地在键盘上不断地敲出一系列的软件程序，大学三年级时与扎克伯格一样从哈佛大学辍学；31岁时他让那些软件程序帮助自己成为亿万富翁，在《福布斯》全球巨富排名榜中，他从1995年起到2007年一直雄踞榜首。

盖茨1973年进入哈佛大学攻读法律，但是命运没有让这个世界上多一个品学兼优的学生，而是鬼使神差地造就了一个电脑天才。1975年盖茨离开哈佛，与好友保罗·艾伦共同成立了微软公司，并在31岁成为有史以来最年轻的亿万富翁。

鉴于盖茨对整个世界做出的卓越贡献，哈佛大学破例将盖茨视为1977届哈佛毕业生并授予他荣誉法学博士（L.L.D）学位证书。哈佛大学德里克·博克校长在介绍盖茨时不吝赞美之辞："我们今天的演讲者是世界上最具影响力的企业家，他带动了个人计算机行业的革命。从2004年到2007年，他连续四年当选'全球100位最具影响力人物'。"随后，他以开玩笑的口吻对盖茨说："如果你当初完成剩下两年的学业，那现在将取得什么样的成就呢？"

盖茨的演讲也非常诙谐，他说："我一直对我的父亲说我会继续回到哈佛翻那些书本，以便拿到自己的学位，现在我做到了。为了说这句话，我等了30年。有了这本证书，我想我终于可以跳槽到一个看上去比较好一些的公司里去了。"

哈佛大学校刊《哈佛深红报》曾将盖茨称为"最成功的辍学生"。

B. 史蒂夫·乔布斯

在扎克伯格出现之前没有人会否认苹果公司执行总裁史蒂夫·乔布斯是紧随比尔·盖茨其后的第二个传奇。在入读俄勒冈州的里德学院6个月后，因为家中贫

困，乔布斯不得不离开学校。在接下来的两年多时间里，乔布斯在一个地下车库中手工拼制出第一台电脑，并开始向自家周围的住户们推销他的产品，他最终创立了为世人所惊叹的苹果公司、NeXT电脑公司和给世界带来无尽欢笑的皮克斯动画工厂。

C．鲍尔默

微软CEO史蒂夫·鲍尔默在斯坦福大学发表演讲时表示，他辍学进入微软工作曾遭到父母的激烈反对，而这差点毁掉他这个现在的亿万富翁。

附：历史上最牛的演讲——甲骨文总裁拉里·埃里森（Larry Ellison）在耶鲁大学的演讲。

耶鲁的毕业生们，我很抱歉——如果你们不喜欢这样的开场白。我想请你们为我做一件事。请你好好看一看周围，看一看站在你左边的同学，看一看站在你右边的同学。

请你设想这样的情况：从现在起5年之后，10年之后或30年之后，今天站在你左边的这个人会是一个失败者；右边的这个人，同样也是个失败者。而你，站在中间的家伙，你以为会怎样？一样是失败者。失败的经历，失败的优等生。

说实话，今天我站在这里，并没有看到一千个毕业生的灿烂未来。我没有看到一千个行业的一千名卓越领导者，我只看到了一千个失败者。你们感到沮丧，这是可以理解的。为什么我，埃里森——一个退学生，竟然在美国最具声望的学府里这样厚颜地散布异端邪说？我来告诉你原因。因为我，埃里森，这个行星上第二富有的人，是个退学生，而你不是。因为比尔·盖茨，这个行星上最富有的人——就目前而言，是个退学生，而你不是。因为艾伦，这个行星上第三富有的人，也退了学，而你没有。再来一点证据吧，因为戴尔，这个行星上第九富有的人——他的排名还在不断上升，也是个退学生，而你不是。

你们非常沮丧，这是可以理解的。

你们将来需要这些有用的工作习惯，你将来需要这种“治疗”。你需要它们，因为你没辍学，所以你永远不会成为世界上最富有的人。哦，当然，你能以你的方式进步到第10位、第11位，就像史蒂夫（此处指微软CEO史蒂夫·鲍尔默）。不过，我没

有告诉你他在为谁工作，是吧？根据记载，他是研究生时辍的学，开化得稍晚了些。

现在，我猜想你们中间很多人，也许是绝大多数人，正在琢磨“能做什么，我究竟有没有前途？”当然没有。太晚了，你们已经吸收了太多东西，以为自己懂得太多。你们再也不是19岁了。你们有了“内置”的帽子，哦，我指的可不是你们脑袋上的学位帽。

嗯……你们已经非常沮丧啦。这是可以理解的。所以，现在可能是讨论实质的时候啦——绝不是为了你们，2000届毕业生。你们已经被报销，不予考虑了。我想，你们就偷偷摸摸去干那年薪20万的可怜工作吧，那里的工资单是由你两年前辍学的同班同学签字开出来的。事实上，我是寄希望于眼下还没有毕业的同学。我要对他们说，离开这里。收拾好你的东西，带着你的点子，别再回来。退学吧，开始行动。

我要告诉你，一顶帽子一套学位服必然要让你沦落……就像这些保安马上要把我从这个讲台上撵走一样必然……

（此时，拉里·埃里森被带离了讲台。）

——第六章——

虚拟世界的普罗米修斯：为资源共享而战的黑客殉道者

你曾是我们中最棒的一个；愿你能够激发我们的无限潜能。

——黑客组织Anonymous在麻省理工学院网站主页上的留言

❶ “mit.edu已失控”

2013年1月14日，星期一。天阴沉得吓人。连续多日的降雪给原来就拥堵不堪的道路又添了不少麻烦，赶着上班的车子像游乐场里的碰碰车，一路跌跌撞撞伤痕累累地赶到公司后，刷卡机上还是经常会遗憾地说“对不起，您已迟到”。

麻省理工学院的网络工程部主管阿卜杜·欣吉气急败坏地走进办公室，一路上他的车被三辆车剐蹭，但他还是甘愿息事宁人赶到公司来，他宁愿自己掏腰包修车也不愿耽搁工作。“最近太乱套了。”

是够乱的。不仅仅是天气，整个世界都疯了。

阿卜杜·欣吉坐下来，望了眼桌上的咖啡壶。往日的习惯，他会先用女朋友从荷兰带回来的纯正的咖啡豆磨一壶浓香的咖啡，只可惜这几天连

续的熬夜，咖啡豆消耗殆尽，包括他的好心情。

随后视线转向电脑的他，被惊呆了。

旁边的监视器上，本应该显示着麻省理工学院的主网站首页，淡黄色的背景下整个网站的格调很娴静，像位中世纪的淑女。只是，现在的监视器上怎么红彤彤的一片？

他揉揉眼睛，把身子凑过去。没错，网站的首页被一片猩红覆盖着，屏幕的下方，有一行提示语：

“不论信息存储何处，我们将义不容辞地获取信息，建立备份，与整个世界共同分享。我们是自由联盟的游击队，我们将按照民间起义的模式，表达对公共文化盗窃的抗议。”

这段话很熟悉，似乎在什么地方读到过。只不过，阿卜杜·欣吉的脑子已经被太多的信息塞得忙不过来了。他点起一支烟，正要拨个电话让他的助手迪莫过来，迪莫已经连敲门都省略了，旋风一样冲进来，手里捏着几张纸，“欣吉主任，我们的网站被黑了。据不确定的消息，黑客来自一个名为Anonymous的黑客组织，这是Twitter[①]上的截图。”

迪莫把手中的打印纸递过来，上面是一个网页的屏幕截图，图上是一个名为Anonymous发布的消息，短短的一句话：“mit.edu（麻省理工学院的网址）已失控。”

“Anonymous我听说过，也不是什么很严密的黑客组织，他们和我们之间有什么过节吗？”

“我想让您再看看这句话。”迪莫用手指着被黑的网站首页的屏幕下方的提示语。“这句话您应该还记得，这是信息游击队自由宣言中的一段话。这个信息游击队的发起者是斯沃茨。”

① Twitter是美国最大的社交网络及微博客户服务的网站，允许用户将自己的最新动态和想法以手机短信的形式发布，其口号是Share and discover what's happening right now, anywhere in the world!（现在发生了什么，我们一起分享和发现，无论在世界的任何地方！）在美国，前一秒钟发生了什么，你保证可以在Twitter上搜索得到。

阿卜杜·欣吉颓然地坐回到椅子里，“我原以为斯沃茨已经死了，一切都已结束了。”

迪莫呆呆地望着被改得一塌糊涂的网站首页，深深地叹了口气：“也许，一切才刚刚开始。”

❷ 数字游侠

亚伦·斯沃茨（Aaron Swartz），1986年出生，斯坦福大学计算机专业的辍学生。与他的同龄人马克·扎克伯格、上文刚刚提及的Twitter的创办人杰克· 多西相比，斯沃茨显然乏善可陈。但是，上天注定要这个平凡的年轻人做出不平凡的事情来。

怎么说，斯沃茨都可以算作个天才，在14岁的时候就已经被聘任参与制定Rss1.0规范，这是个足可以称之为伟大的工程。随后斯沃茨创办了自己的软件公司Infogami，几经辗转，Infogami先是与Reddit（红迪网）合并，继而被卖给了美国传媒巨头康泰纳仕集团。2007年1月斯沃茨从康泰纳仕集团辞职，受聘在哈佛大学研究中心担任研究员。

多年的IT界打拼，斯沃茨看透了门户之争、各自为战的IT界和被专利和版权束缚的思想和技术。原来，世界上除了飞鸟，IT界的才智们也需要高飞的翅膀。

就像跳水的台子，搭得越高，越能做出漂亮动作。

2000年，斯沃茨参与创建了一个名为“要求进步”（Demand Progress）的纯民间呼吁组织。这个机构有着明确的目标，那就是通过互联网手段，针对特定的敏感议题向国会议员及政府相关部门传达意见、施加压力、公布结果。该组织在反对《禁止网络盗版法案》（SOPA）和《保护知识产权法案》（PIPA）的战斗中非常活跃，一时之间成为美联邦中自由共享组织的领导核心。

在忙着制定Rss1.0规范的同时，斯沃茨发现《禁止网络盗版法案》和《保护知识产权法案》的相关条款与其他法律有内容上的重叠和冲突之处，而当他想进一步搜索相关的法律条文时，却被网络通知，必须注册并交纳一定的阅读费用才可以使用相关的内容，这让斯沃茨极为不满。美国法庭电子记录公共接入服务（PACER）是美国最完整的法律资源库，该服务提供联邦司法案件的存档，每篇文档收费10美分。斯沃茨认为这些非涉密性的文件应该共享并免费提供给公众使用。斯沃茨随即编写了一个小程序，通过系统自动注册，并将这个新注册账号的权限提升到管理员级别，然后用管理员的身份从该服务中心下载了2000万页相关的法律文档挂载到网络上供全世界的人阅读。这些资料占整个数据库资料总量的20%。

鉴于斯沃茨此举并未对网络系统造成破坏，且公布的文件也不含机密，而且没有实质性的盈利目的和行为，美国联邦政府虽然传唤了斯沃茨并对这一事件进行了细致的调查，但并未对斯沃茨的行为起诉。

通过这一事件，斯沃茨渐渐开始成为英雄，他被业界称为“数字游侠”，无论在黑客行业还是正统的IT界，斯沃茨都拥有众多的支持者，他们用网络做纽带，呼吁网络信息自由开放，而不是通过收费来阻止信息的自由交换并从中谋利。在此基础上，斯沃茨提议并成立了知识共享（Creative Commons）组织，该组织致力于推动有关社会公平问题的网上行动，例如阻止由好莱坞支持的互联网隐私保护法立法。

❸ 50年监禁与400万罚款

知识产权、著作权法和资源共享的矛盾有多深，来看看网络上的盗版与反盗版之争吧，看一看那些需要注册交费才能下载和使用的网站吧。相信每个人都遇到过类似的情况，搜索到自己需要的信息，点击下载时，会要求注册和支付费用，维普资讯网、中国知网、吾喜杂志等网站都是这种

经营模式。只提供你阅读信息的一小部分内容，若是你觉得有用，想得到完整的信息，对不起，请付费。

这很有些当年的共享软件的风格。共享软件会限制未注册者，他们只可以使用软件的一部分功能而不是全部，如果感觉需要其他功能，就需要注册和交费，类似于走街串巷小贩们的“先尝后买”。

斯沃茨便想在自由和共享上做侠之大者，在“保留所有权利”和“不保留任何权利”之间做出平衡。在尊重原作者利益的前提下，最大限度地发挥资源的共享性和传播性，让资源尽可能地被充分利用起来而不是成为某些人的牟利工具。而现实的状况是，全世界所有科学与文化、古籍和每天更新的报纸杂志的内容，正在不断被扫描转化成数字，被政府和少数私人机构“垄断”并以此牟利。“信息即权力。但是，与所有的权力一样，有人希望将这种权力据为己有，而我的任务是让这幻想破灭。”

2011年，斯沃茨和他的知识共享组织把目光瞄上了美国最大的公众信息资源库——美国期刊数据库JSTOR，而这个数据库的主机就位于麻省理工学院的计算机房。

斯沃茨和他的团队花了半个月的时间研究JSTOR的后台漏洞，并专门针对一些可能被借用的地方编写了入侵程序，直到成功地挂接到JSTOR的后台，并建立了多达十余个超级用户。然后，他们开始疯狂地用这些超级用户登录系统的后台，将大约500万份需付费才能下载使用的资源文件下载，并挂接到知识共享组织的网站上免费发放。

这一举动引起了整个美国的欢呼。

大度的JSTOR似乎并不太在意斯沃茨的举动，也没有打算起诉他的意思，但是强硬的马萨诸塞州法官卡尔曼·奥提兹则坚持起诉，他说：“盗窃就是盗窃，无论你使用计算机命令还是撬棍，无论盗窃目标是文档、数据还是钱。盗窃如不严惩，世界必会大乱。”

调查署对斯沃茨提出了多达13项的黑客行为重罪指控，如果斯沃茨被认定有罪，他将面临最多50年监禁与400万美元的罚款。

4 这不是一个人的悲剧

最终，斯沃茨还是没给法律一个制裁他的机会。2013年1月11日，在交了10万美元保释金回到家中后不久，斯沃茨用一根绳子给了自己一个了断。

在自杀之前，斯沃茨最后一次打开电脑，在美国最大的文件分享网站“海盗湾”上投放了一个BT种子文件，包含18592篇文章，BT包大小为32.48GB。“我一个人抵抗不住全世界的打击，不过，我还是要谢谢你们的欢呼和鲜花。顺便说一句，学术论文本应该允许自由获得，但是大多数论文都被JSTOR这样蹩脚的守门员以高额收费的形式阻止传播。这些本该属于公众领域的信息资源被束之高阁，是对知识的浪费。把属于公众的东西还给公众，我这样做有错吗？这些论文，应该对所有人免费。这是我最后一次这样做了。”落款是，永远爱你们的亚伦·斯沃茨。

事实上斯沃茨不止一次地谈到过死亡。早在2007年，在一次记者招待会上，他就公开声称“如果有一天我消失了，我想我是死在为自由而战的冲锋路上，而这不是一个人的悲剧”。

当年参与创建“要求进步”的民间组织时，斯沃茨也不止一次地提到过自己被慢性胃炎无休止地折磨着，同时折磨他的还有挥之不去的压抑感。“出去呼吸新鲜空气，与相爱的人共处，这些不会使你感觉稍好，只会更失望。你无法感受到其他人的快乐，所有事情都令人悲伤，你能感觉到痛苦的痕迹在你脑海中流动。你虐待自己的身体，希望逃离，但是做不到。这还只是较轻的症状。无论如何，这世界不是我希望看到的样子，也并不符合我的理想状态，我想，这是我所有病症的根源。”

与维基解密的阿桑奇一样，斯沃茨是一个信息自由主义者，他们都在用游侠般的豪情和破坏性的动作，做着一件除暴安良、替天行道的大事。

斯沃茨的自杀成为各大门户网站的头版头条，随后而来的是铺天盖地的大讨论。有关自由、有关版权、有关收费与免费、有关伦理与尊严。

斯沃茨的良师益友、著名的法学家、律师劳伦斯·莱斯格在自己的主页上以“检察官是法律的暴徒”为题洋洋洒洒写下数千字，一针见血地指出“如果政府的指证是真的，那么斯沃茨确实做错了。如果不是法律上的错，至少也是道德上的错，是行事方法和手段上的错。但是，法律的苍白在于没法做到合适的惩罚。他是一个恐怖分子吗？他是一个试图从偷窃的物品获益的破坏者吗？斯沃茨‘盗窃的资产价值数百万美元’，这些措辞意味着他的目标是从犯罪中获利。但是，谁要是认为能够拿一堆学术论文赚钱，他要么就是疯子，要么就是在说谎”。

更多的人则喜欢用最直接的方式表达自己的不满，和对斯沃茨自杀事件的态度。继麻省理工网站被黑之后，美国司法部、联邦第十三检察署等网站接连被攻破，JSTOR网站连续一周被黑客狂轰滥炸。国际著名的黑客组织Anonymous闯入美国司法部下属的独立机构美国审判委员会的网站，并通过一段视频威胁说斯沃茨因受不了当局的逼迫而自杀身亡，Anonymous组织认为美国的司法机构已经“越过了法律和人道的双重界限”。他们此举就是为了伸张正义，为自由的斯沃茨昭雪。

“斯沃茨不光对我们非常失望，也同样对自己和这个世界失望。他无力挣扎，于是，他用死来摆脱这种无济于事的挣扎。”想凭一己之力与整个世界抗衡，这本身就是错误，虽然，错得这样美丽。斯沃茨死了，有关斯沃茨的故事还没有结束，有关自由版权的讨论才刚刚开始。著名科幻小说家，同样是斯沃茨的朋友多克托罗说得正确：“他只不过是通过自己擅长的方式，诠释了黑客精神的根髓，并通过他认为正确的方式，为自由这个名词做一次身体力行的告别演出。”

❺ 一个黑客的三大战役

与斯沃茨26岁的年轻相比，乔纳森·詹姆斯在通往天堂的路上更显得

迫不及待。比斯沃茨大3岁的詹姆斯，在2008年5月18日“因癌症去世，享年25岁”。

这个有史以来位列黑客名人榜第四位的超级黑客的死因，似乎被医院的一纸死亡证明盖棺定论，而实际上，他的好朋友艾德里安·拉莫的话似乎可信度更高一些：詹姆斯用一把手枪，给自己的脑袋来了个漂亮的十环。

用声名狼藉来形容詹姆斯也不足为过吧，可偏偏他又赢了那么多花环和欢呼。他几乎成了神的代名词，“只需要动一动手指，全世界都不再有秘密可言。”这句话，只有放在他身上才不会有任何人怀疑。

可是，究竟什么原因，让这个25岁的天才能忍得住寂寞，却与死亡亲密接触？

1999年，那时候詹姆斯还是个初中生，刚刚普及的互联网还不十分健全，这给了詹姆斯极大的活动空间。天生对数字敏感的詹姆斯只要一摸到键盘就忘乎所以，他没上过任何计算机辅导班，却编得出极其严密简洁的程序。从街边的电话到家里的黑白电视，他都可以用一台电脑加几行代码就随意控制。

直到有一天，居然让他找到了OTRA的一个漏洞。

OTRA是美国国防部下属的一个核化、生化等特殊武器的研发机构。詹姆斯误打误撞地在OTRA的中继服务器的某个节点上，找到了一个没有修补漏洞的路由器并成功地控制了它。然后，詹姆斯以这个路由器为中转，在其中埋设了木马程序，拦截了超过4000个发往OTRA的工作数据包，同时也拦截了OTRA的员工进出记录和密码，这其中包括至少8个拥有最高权限的超级用户密码。

这一年的6月29日和30日两天，詹姆斯分两次使用代理服务器把自己的真实IP挂接到西海岸某个学校的终端上，然后用超级用户登录OTRA的主服务器，下载了来自美国国家航天事业部和航天局价值约200万美元的专用软件，同时把相关的国际空间站的运行规范手册等绝密资料翻了个底

朝天。这一举动历时不到20分钟，成绩是让美国国家航空和航天局的计算机系统被迫关闭21天，损失过亿美元。

幸好在詹姆斯还没有找好买家之前，FBI已经抓到了这个年仅16岁的天才儿童，虽然詹姆斯一口咬定只是因为好玩和刺激，并没有考虑经济收入，但鉴于“绝密软件和资料的外泄事件必须杜绝”的杀一儆百的理由，詹姆斯被判处6个月监禁。

莫里斯蠕虫（Melissa）救了詹姆斯。1999年，这个因程序代码编写错误造成的蠕虫病毒在几个小时之内横扫全球，致使整个互联网的电子邮件系统崩溃。当局一筹莫展、袖手无策时，詹姆斯成功地在蠕虫病毒的代码中搜寻到了病毒制造者莫里斯的信息，并协助FBI将莫里斯抓捕归案。

鉴于詹姆斯在反病毒中的杰出贡献，当局决定撤销他6个月监禁的处罚，并允许他进入大学深造。要知道在美国，有犯罪前科是很难进入大学的。

随后的2000年，爱虫病毒肆虐全球，FBI又想到了正在大学深造的詹姆斯，而詹姆斯也不负众望，在一周的时间里再次揪出了病毒的来源，一时间业界称雄，光芒四射。

❻ 突破界限的根本

两个漂亮仗加一次成功的入侵，让詹姆斯成为黑客界的顶尖人物。而有别于一般黑客，詹姆斯更侧重于以黑客手段公开一些加密的隐私资料，以及需要付费才能使用的信息源。

“我相信互联网时代没有什么是不能共享的。互联网应该是一个各取所需的工具，而不是致富手段。”

大学毕业后，詹姆斯成立了一个非营利性的民间机构，用以挖掘整理互联网上的共享资源，将它们有机地整合成一个体系，建立目录供浏览者

使用。只是这工程太庞大了，他不得不呼吁所有使用互联网的人一起动手来做这件事情。与此同时，他瞄上了美国国家信息局的数据库系统和英联邦的国事图书馆在线查阅系统。这些数据库内容丰富、目录详尽，只是其中很多内容需要注册后付费使用。而詹姆斯的愿望则是冲破这种视金钱为上帝的壁垒，带着自由共享的翅膀打造一个纯净自由的网络世界。

针对这两个数据库的底层代码，詹姆斯通过无数次的侦测和实验，亲手编写了两个对应的潜入程序，分别挂接在两个服务器上。其编程思路是，只要有付费用户浏览或下载了那些需要付费的内容，程序便会自动进行链接，从后台直接把那些未经付费无法阅读的内容直接拉到本地计算机上。这相当于主人打开了冰箱，刚取了面包，还没来得及拿果酱时，旁边淘气的孩子已经借机去翻苹果了。

长达两个月的时间里，詹姆斯获得了大约7000万字需付费才能使用的资料，然后分门别类地挂接到自己的免费网站上无偿供用户使用。

“黑客的精髓在于打造一个完全自由民主的网络体系，而不是捣蛋。那些出卖技术换取金钱和声望的黑客，应该被驱逐出这一神圣的领域。而我，会一直为自由而战。这是我理想中的自由根本。”詹姆斯对于随之而来的法律指控不以为然。“如果我一定要坐牢的话，16岁那一年我已经坐了。法律上的‘盗窃’是以经济为目的的巧取豪夺，我所做的一切干净得像自来水，你能闻到这其中有铜臭气吗？”

詹姆斯的行为无疑让法律抓狂。现行的法律真的对他无能为力，这让法官们很难堪，甚至在国会的压力下试图尽快修改属地法律来惩戒这些不法之徒。而黑客集团和倡导自由的人士，则把詹姆斯奉为不败的斗士、传奇般的佐罗。

虽然光芒四射，其实詹姆斯的日子并不好过。与FBI的合作类似于“警民共建”，基本上是义务的无偿劳动，而作为一个高精尖的黑客奇才，又有哪家机构肯收留这样一枚定时炸弹？

事实上，詹姆斯一家吃饭都成了问题。他每天忙于收集整理那些免费发放的资源，过着朝不保夕、食不果腹的日子。他握着高深的黑客技术，却洁身自好不做损人利己的勾当。他扯着自由共享的大旗四处碰壁。甚至当他去楼下的超市应征做搬运工时，超市的老板居然说："这个自由共享的先生，可不可以这样，你不要报酬，把劳动所得共享给公众？"

2006年秋，詹姆斯终于再一次展现了精湛的入侵艺术。他侵入了一家计算机安全公司的主机，把电脑的桌面改成了他自己的照片。"我只是想告诉你们，我需要一个工作，而计算机安全是我的强项，我唯一的要求是月薪50美元。"

这家不出名的计算机公司最终还是录用了他，主要职责是给公司开发的软件挑错找漏洞，只不过他做了两个月就辞职了。在他眼里，这家公司的产品简直就是垃圾。

一方面他拥有着世界顶尖的黑客技术，一方面无偿发布着互联网上的免费大餐，而他自己连吃顿饱饭都是奢侈。"在和金钱较量的过程中，热爱自由的人不一定会输，但是想赢，也几乎是不可能的。"

绝望的詹姆斯，于是不知从哪里搞到了一把枪……

与黑客们崇尚的自由民主和平等的态度来打量这世界，显然世界被人为地分为三六九等，甚至在阅读权限上都体现出VIP的优越性。一向标榜自由的黑客们对等级森严的网络不屑一顾，并试图通过自己的手段和方式达成二者的共融。只是，如何区分机密与共享？如何为资源的整合工作提供更好的服务，而随着这服务产生的人工费、服务器存贮费等相关费用又如何计算，完全共享的回报又在哪里？很多现实的问题不是一两句话就能解释清楚的，于是，矛盾出现了。

黑客喜欢用最直接的方式达成最终结果，他们很少考虑问题以外的其他因素。执着得可爱，又调皮得可恨。

可是，谁又能说，这样的黑客，不是让公众欢呼鼓掌的？

【黑客知识】

RSS：简易信息聚合技术的统称，是一种描述和同步网站内容的格式。在新闻网站上使用RSS订阅能更快地获取信息，网络用户也可以在个人电脑上借助于支持RSS的聚合工具软件，在不打开网站内容页面的情况下阅读支持RSS输出的网站内容。

数字化阅读：美国《时代》周刊前主编沃尔特·艾萨克森曾预言，在互联网时代，传统的零售、订阅和广告报刊经营模式，将不可避免地被网络付费阅读、网络广告的商业模式所取代。如今，他的预言正在变为现实。国内的起点中文网等多家网站都已开始实行收费阅读，除了原有的大量免费阅读内容外，还建立了创作、培养、销售为一体的电子在线出版机制，内容从期刊内容到各种小说、戏剧、国家法规及一切可能收集并对公众有意义的文字图片素材。网络把图书馆式的包容量与我们日常生活拉得更近。

——第七章——
道与魔的较量：病毒猎手

我的目的不是赚钱。金钱好似氧气，足够多当然好，但不是目标，目标应该是拯救世界。

——俄罗斯信息安全专家尤金·卡巴斯基

❶ 截获“Flame”

2012年5月，日内瓦。联合国国际电信联盟秘书长哈马德·图埃的办公室里，图埃将一叠报告交到两小时前刚刚降落的卡巴斯基实验室首席执行官、俄罗斯网络安全专家尤金·卡巴斯基手上。“我们急着找到您，是因为像两年前Stuxnet蠕虫病毒那样，伊朗方面石油部门的机密信息正在被未知但确定存在的木马程序窃取。”

两年前，总部位于莫斯科的卡巴斯基反病毒实验室检测并成功地排除了世界首个网络“超级武器”Stuxnet蠕虫病毒[①]，当时这个病毒曾使布什尔核电站的离心机因程序受损而推迟装填核燃料。此番病毒袭击再次针对伊朗，图埃希望卡巴斯基能再显身手。

卡巴斯基在哈马德·图埃的办公室里连入互联网，召集了属下的反病

① 可参见《会越狱的苹果》一章中的黑客知识。

毒精英，要求他们在两小时内彻底清查全球“卡巴斯基安全网络”成员发送来的疑似病毒样本记录，重点放在中东地区。随后的几小时内，一个振奋人心的结果出现了，在417台送检的疑似病毒样本中发现了同样的不明临时文件，其中185台位于伊朗，有的机器中这个文件的最早创建时间在2010年，也就是说，如果这是一个新型的潜伏式木马病毒的话，那么其样本早在两年前就已经成型并投入使用了。

经过长达一周的代码分析，卡巴斯基实验室将这个病毒命名为“Flame”，到目前为止，该病毒是这个世界上功能最健全的反病毒实验室遇到的最为复杂的间谍软件。它捆绑了系统进程，让常见的杀毒软件认为它属于一个系统必备的关键进程从而对它放行，其代码长度达到了惊人的6万行，堪比一个小型的操作系统。其编程手段高超，具有极强的反查杀能力和自我修复能力，并具有极高的间谍功能，绝非一般黑客所能编写的，也不是一两个人在短时间内就可以完成的庞大工程。几乎可以断定是某一政府授意制造，并且很可能与早先发现的Stuxnet病毒具有同样的目的：侦测并收集伊朗相关的石油机密数据。

2012年6月1日，《纽约时报》首次公开承认美国白宫曾在几年前有组织地对伊朗发动了一场网络间谍战，Stuxnet是整个计划的一部分；6月19日，《华盛顿邮报》也发文证实，Flame是在Stuxnet基础之上的第二个版本，也是这场秘密战的重要组成部分，早在几年前便通过各种可能的途径渗透到伊朗相关的计算机系统之中去了。

❷ “那是高级机密，所以我不记得了”

两次针对伊朗的国家级黑客行动被一个数十人的精英团队斩落马下，美国人感觉很没面子，一边忙于否认，一边用重金贿赂这个组织的领导者

尤金·卡巴斯基，而后者只报以一笑，并不为之所动。

尤金·卡巴斯基，天生对数字有着超强的理解能力和运算能力，16岁被招入一所“不宜公开的”有着克格勃背景的电信密码专业学院学习，毕业后进入军方。有关这一段记载，以及他在学校和军队里的那些年都做了什么，在他的履历上也是只字不提，用他自己的话说，“那是高级机密，所以我不记得了。”

不记得就不记得吧，这并不影响我们理解这样一位业界超人，甚至，只有这样才更有神秘的意味。总之，这位背景颇深的情报人员一出场就注定与机密、电脑、情报这些字眼联系在一起。

第一次接触电脑病毒是1989年秋天，卡巴斯基的电脑屏幕上突然出现了两个乒乓球样的东西不住地滚来滚去，只要碰到显示的字符就把它“吃掉”。当时他只觉得这很好玩，并没有意识到这是病毒，于是他把电脑硬盘上的数据统统备份下来，再重新用一块新的硬盘安装上去，并安装了与原来的硬盘相同的软件，这样，两块硬盘便在理论上有着完全一致的文件了。卡巴斯基将新硬盘的文件目录和文件长度打印出来，与原来那块硬盘上的数据作对比，找出这个病毒可能感染的文件并将之剔除。再打开其内核仔细研究一番后，他针对病毒特征编写了一个可以自动侦测病毒并剔除程序的软件。这样当第二次“遭遇毒手”的时候，他就不用手工操作了，“我只需要冲杯咖啡，在键盘上按几个键，敲一下回车就行了。”

随后计算机病毒大面积发作时，卡巴斯基每当遇到一个新病毒都要不吃不喝，几十个小时在电脑前反复检查和筛选，直到把病毒清理干净，然后将得到的特征码加入到自己编写的软件中去。很快，这个可以清除病毒的软件开始被竞相复制和使用，而卡巴斯基这个名字也水涨船高，成为小有名气的反计算机病毒战士。

接下来的两年时间里，卡巴斯基沉迷于反病毒工作中乐此不疲，甚至打算脱下军装从事职业反病毒工作，但这几乎是不可能的，因为他的机密

身份和涉密的工作性质不允许他随便成为普通百姓。

他找到了一位在政界活动能力超强的电信密码专业学院的导师，在这位导师的帮助下，他终于顺利地脱下了军装，作为回报，他加入了这位导师的公司并从事职业的编程工作。当然，这位导师用了什么方法达成了他的愿望，这依然是不能说的秘密。

❸ 目标应该是拯救世界

1997年，卡巴斯基脱离了这位导师，与妻子娜塔丽娅成立了属于自己的病毒实验室，并推出了以自己名字命名的全新一代杀毒软件，在短短的几年时间里，市场份额就达到了惊人的3亿用户。更难能可贵的是，由他创立的世界级的病毒代码特征库已成为反病毒业的标准测量试验库，也就是说，每一种杀毒软件的实际杀毒效果如何，要经过卡巴斯基测量试验库放出的带有病毒样本的程序文件的检测。更通俗的解释是：一个杀毒软件“可以打多少分”，要拿来由卡巴斯基评定，在计算机里投入一个含有成百上千种病毒样本的文件，让这个杀毒软件来查杀，用“可查杀数”除以“文件中包含的病毒数”为最终得分。

这是对这个退伍军人最高的奖赏。而雄心勃勃的卡巴斯基声称，自己要靠一套软件拯救世界。

是不是能如他所愿还不知道，但是他仅凭一套软件就赢得了计算机界最高的荣誉这倒是真的，而且，这套会下金蛋的软件，也的确打造了一个亿万富翁。

对于卡巴斯基——这个身份最神秘的计算机大亨，我们只知道这么多。

❹ 草根英雄——王江民

与卡巴斯基相比，王江民就显得草根得多。

自从360杀毒和金山毒霸分割了国内杀毒软件市场之后，在中国境内，连卡巴斯基这等国际级的杀毒软件也占不了便宜。

若是王江民还在，杀毒软件的江山落入谁手还未尝可知。

2010年4月4日，在京西信翔鱼池钓鱼的王江民因突发心脏病，抢救无效，于上午十时去世，享年59岁，遗体于当月8日在八宝山革命烈士公墓火化。

当日，国内各大杀毒软件商的网站首页均改为灰色，以示悼念。

王江民的名字已经淡出了中国计算机界的视线，但在某些人的心目中，“王江民”三个字代表着一种英雄主义的传奇。

38岁之前甚至没有接触过计算机，却是北京中关村最富有传奇色彩的业界领袖、民营企业家、中国软件业的奇才、国际知名的杀毒王。他一生全靠自学，获得过20多项专利，更是一位社会公益事业的带头人和慈善家，先后向国家残联以个人名义无偿捐款近200万元。

这个人就是王江民。

他是著名的反病毒专家，国家高级工程师，烟台市政协委员，山东省残联协会副理事长，中国残联理事；同时，他还是北京工业大学教授，辽宁对外经贸学院教授，国家信息技术安全指挥部特聘专家；他的荣耀称号有新长征突击手，自学成材标兵，全国自强模范。

可是，这样一位传奇人物，却是个小儿麻痹症患者，终生残疾，连高中都没有上过，从未接受过任何正规大学的教育，十几岁在一家街道小厂做工人，一干就是20年。

❺ 独闯中国硅谷

3岁，刚刚记事，小儿麻痹症就夺去了王江民的一条腿。“我自己无法下楼，只要一踏上楼梯，就会从楼梯上一直滚下去。无论我多努力，从小到大，没有成功过一次。”别的小朋友都在院子里跳绳、荡秋千，享受阳光的时候，他只能倚着窗子，看楼前楼后的燕子衔草搭窝。他还认不了几个字，每天把印着“到农村去，到广阔的农村去”的报纸撕成一条条的纸带，折一下，丢到窗外，看那些纸条打着滚满世界飘。

不会下楼的王江民却学会了骑自行车，这对他来说是个天大的喜事。小学四年级的时候，那条不给力的腿又被自行车轧断了一次，不服输的他于是和自行车较上了劲，在不止一次摔得鼻青脸肿之后总算学会了；因为腿不好使，虽然生在海边，他却只会憋住一口气，一个猛子扎到水底，能游多远算多远，在灌了很多次海水之后，终于也学会了抬头游泳。在被自行车轧断了腿不得不在家休养的那段时间里，他连去窗口撕报纸条的权利都被剥夺了，却咬牙拼出了十六个晶体管的收音机和无线电对讲机。

“初中毕业后，家里条件困难，决定不上高中了，可是找不到工作。不要工资，白干，就图个长经验，人家都不要，嫌我腿脚不好使，碍事。”王江民自学了一年多针灸，试图治好自己的腿，但是十多年的旧疾，仅凭几根银针显然于事无补。他拿着自己拼凑的电子收音机挨个工厂敲门。“看，我的腿虽然不好，但我有能干的双手。”

1971年，终于有一家街道工厂愿意接收他。他喜出望外，拼命工作，不出两年就成了厂里的骨干。1978年，王江民申请激光治疗仪器专利成功，只有初中文化的王江民被评为全国105个新长征突击手标兵之一。“这是最好的奖励了，至少一个残疾人，可以成为中国的一百零五分之一。”

1987年，王江民的光投影万花枪专利申请成功；1992年，球轴承自动

装配线获烟台市科技进步二等奖……一个个国际级的科研成果，一个个国家级的奖项，让拖着一条残腿的王江民终于挺直了腰杆。

1988年，已经是国内机电行业小有名气的王江民开始接触工业控制系统，光电自动化必须由计算机控制，不学计算机肯定不行。38岁，王江民花了三个月的工资买来一台中华学习机，开始自学BASIC语言，第二年又换成一台带有DOS操作系统的8088电脑。

编程讲求实用性，光靠教材上的例题显然不行。当时王江民的孩子正上小学，老师给家长的任务是每天给孩子出五十道数学题。正在研究编程的王江民顺手编了个软件，让电脑帮忙出题，打印出来让儿子做。后来索性按照教学大纲把小学初中的教材内容都做成软件——这个软件在国内著名的计算机报刊《电脑报》发起的交流中被评为第二名，而第一名正是金山公司的WPS。

《电脑报》每套软件卖出后会给王江民25元，最后王江民靠这套软件挣到了1000多元。这是从学计算机开始，王江民得到的第一笔回报。

在光电控制中，王江民主要负责相关的软件开发，但经常会遇到用户抱怨说软件不好用，经常出错。王江民经过检查，发现程序被修改过。那时候还不知道这就是病毒，于是他开始分析自己编写的程序与用户电脑中软件的差异，并手工剥离出病毒代码。当计算机界开始将注意力转向计算机病毒时，王江民已经积累了很多杀毒的具体方法和技巧。为了让更多的人认清病毒，每当他捕捉到一个病毒样本后，就会在报刊上公布这个病毒的特征码，以方便有能力的电脑使用者自己修补电脑。最后，王江民决定把目前已知的多种病毒代码整理到一个固定的程序中，以便普通电脑用户也只需要执行一下自己的程序就可以杀灭这些病毒。最初，他把这个软件定名为KV6。

在最终这个定名为KV6的软件中，王江民把主程序和病毒特征码分为两部分，主程序调用一个可以手工人为输入特征码的、有固定格式的文本文件。以这个文本文件中的病毒特征码为依据在用户的计算机中搜索病

毒，这样，只要简单地扩充这个病毒特征库，就可以无限制地增加可以查杀的病毒数量。这一编程思路一直贯穿在KV杀毒软件的整个研制和发展过程中，后来这种方式也成为国内很多杀毒软件公司采用的一种非制式规范。

1994年年初，王江民将KV软件升级至KV100，并按照国际规定（不能全部用数字来命名软件）将其命名为“超级巡警”，同时交给《电脑报》再次交流，并与《电脑报》联合，在报纸上开了“反病毒公告”专栏，定期公布最新的广谱病毒特征码。在没有网络和光盘的阶段，因为病毒特征码，《电脑报》的销量剧增，同时带动了KV软件的销量大幅度提高，真正做到了双赢。

光靠病毒特征码和报纸，显然还构不成最良好的商业模式。1996年，王江民从单位辞职，一个人来到中关村。

20世纪90年代的北京中关村，聚集着全中国的高新科技公司和最先进的电子科技，几乎所有计算机相关的大公司都在中关村设有办事处或商业销售点。

王江民拿着已经名满天下的KV100挨个公司找代理，从最初的2万元代理费都没有人肯做，到最后一个订单就要成百上千万。王江民跑了三年时间，KV系列软件也从100升级到300。一个患有小儿麻痹的初中生，在一个周围都是博士、硕士的高科技产业园里拼到了最后，终于把KV系列做成了国际品牌。

想想看，光中关村注册的企业就有近2万家，其中做杀毒软件的不下几十家，国内的、国外的，摆在柜台上吆喝的杀毒软件不下百余种，为什么KV却成功了？因为市场需要，因为KV真的好用。几年之内，KV系列的市场占有率超过80%，正版用户超过200万，成为中国正版软件中销量最好的产品。KV被授予“中国名牌产品”称号，多次获最佳软件奖，王江民本人也上了《东方时空》，被北京工业大学聘为兼职教授。按王江民的话说，“一个软件能拿到的奖，我全拿到了。”

一个草根英雄在中国拔地而起。

❻ 从主动逻辑锁到慈善大使

如此过硬的产品，没有盗版，显然就不正常了。

在全力对付病毒的同时，还要对付比病毒狡猾一百倍的盗版，这让王江民伤透了脑筋。

王江民面对的盗版不是破解版，而是带有加密点的伪正版。这种伪正版并没有破坏原版程序，而只对原版程序的加密方式进行破解。也就是说，只破解加密程序而不破解程序本身，程序就会误认为这个软件是正版的，和正版一样享受升级服务，丝毫不影响杀毒效果。

1996年秋，KV300刚刚上市不到一个月，王江民就发现有非正规出品的KV300在销售，因为这些软件的包装盒上印刷的加密条码并没有在江民网站上登记。而这些产品除了在正版的加密程序上又加了一套破解程序，让软件认为这是正版之外，并没有改动任何程序本身的源代码。这是一种非常高级且难度很高的破解。

1997年4月，一个名为毒岛论坛的病毒研究交流网站出现在互联网上，其核心内容不是交流查杀病毒的技术，而是讨论如何解密KV系列杀毒软件。这个网站的解密技术很高超，并有偿提供制作KV300盗版盘的工具软件MK300。

王江民下载了这个可以成批制作伪KV300的软件，仔细分析了其工作原理和破解方式，随后推出了KV300+；毒岛自然不甘示弱，也立即推出了MK300V1，王江民再接再厉更新了加密算法，让MK300V1失效；接下来毒岛也加快了破解速度，接连推出MK300V2和MK300V3，也都被最新版的KV300+一一攻破，如此这般你来我往时间长达半年之久。在MK300推出V4版本之后，王江民一改软件封锁的做法，直接使用了最先进的主

动逻辑锁技术。这个“逻辑锁”的工作原理与查杀病毒很类似，同样是在KV系列软件中查找MK300V4程序的特征码，软件经MK300V4破解过，一旦发现电脑在使用MK300V4给KV300做破解的工作，就会启动逻辑锁把电脑硬盘加密锁住。这一出人意料之举让毒岛论坛用来制作KV300的电脑通通锁死，系统无法启动，更换硬盘后只要一运行MK300程序，硬盘还是会被主动锁死。

至此，在与毒岛针锋相对的半年多时间里，王江民和他的KV300一直占据着主动权，成功地抵抗了毒岛论坛的盗版攻势。

王江民说，在中国，危害最大的不是病毒，而是盗版。一些黑客在针对网络施展其非凡的破坏手段之余，把先进的计算机技术运用到破解正版软件上来，不仅扰乱了市场秩序，也让很多程序员的劳动成果付诸东流。

“主动逻辑锁”事件之后，就王江民这种主动锁住他人硬盘的做法是否恰当，国内软件业展开了一场大讨论。王江民声称，正版KV300的用户和使用没授权的解密版KV300的用户绝不会受伤害，被锁住机器的是那些在大量生产假冒KV300的盗版商。王江民自信“这个逻辑锁就是这样准确”。而有些人则认为王江民和他的江民新技术有限公司为打击“中国毒岛论坛”提供盗版工具MK300V4的违法活动，而在KV300网上升级版中加入保护版权程序，造成使用盗版工具MK300V4的机器死机，属于故意输入有害数据，危害计算机信息系统安全的行为，应予以处罚。

虽然最后此事不了了之，但这无疑是个好广告。经此之后，KV300销量成倍增长，KV300的品牌知名度非常之高，江民公司也从计算机界知名的公司变成了全国知名的公司。

坚如磐石的品质、过硬的技术，使得KV杀毒软件成为世界级的精英产品。江民科技的创始人带着他的传奇先行一步，但江民科技的精神却依旧闪闪发光。2012年6月7日，江民科技正式通过ICSA的反病毒产品认证测试。ICSA测试是国际公认的专业安全产品测试，基于测试结果，江民KV2011成为中国首家通过在Windows7下ICSA测试的反病毒产品。

“江民”这两个字，带着王江民身上挥之不去的坚韧精神，给计算机用户带去了安全感。

【黑客知识】

逻辑锁：逻辑锁是利用了DOS操作系统的一个错误而制成的对计算机底层硬件操作的软件，被锁住之后，无论是用软盘、硬盘，还是光盘、U盘等都不能启动电脑。当计算机通电启动时，DOS系统会自动搜索各个硬件信息，如硬盘、键盘、显示器的类型，逻辑锁则是在系统检测到硬盘的时候，通过修改硬盘的分区表使系统误认为硬盘错误而无法启动。需要说明的是，逻辑锁只针对微软的DOS操作系统有效。

克格勃（KGB）：苏联国家安全委员会。成立于1954年，以强大的侦查实力和高明的破案手段著称于世，是一个凌驾于党政军各部门之上的“超级机构”。它只对苏共中央政治局负责，是“世界上最大的搜集秘密情报的间谍机构”。与美国的中情局、以色列的摩萨德、英国的军情六处并称为世界四大间谍组织。现任总统普京，当初也曾是克格勃成员之一。

——— 第八章 ———

拥有键盘就会对世界造成威胁的人

巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰。

——凯文·米特尼克

1968年夏天的一个中午，天不算晴，但也没有下雨的迹象。午后阴沉的阳光让人感觉慵懒，一个年仅4岁的小孩歪在妈妈的怀里看妈妈摆弄一种“滑铁卢的拿破仑”（类似于中国的华荣道）的棋类游戏。这个年轻的妈妈显然不得要领，十几分钟后就把那破玩意丢在一边转身去逗她的狗了。

儿子看了看妈妈，低头把“拿破仑”捡了起来。“妈妈，这东西最少多少步才能成功？”显然这孩子是看懂了其中的窍门。

“专家的最高纪录是78步。”

“我倒觉得这没什么。让我试试。”

接下来的两天里，这个孩子一声不响地埋头于这种看似极其枯燥的游戏当中。在第二天的傍晚，孩子向妈妈展示了他的劳动成果——只用了83步便完成了游戏。妈妈几乎有点目瞪口呆了：“如果可以的话，你可不可以教教我？”

孩子的回答让他的母亲大吃一惊。“我恐怕没有时间，我准备在一周之内完成最高纪录。”

一周之后，这个孩子在母亲的眼皮底下以78步完成了游戏，然后把那堆木头块丢进了垃圾筒，头也不回地走开了。“我已经完成了，它不可能再快了。”

这个4岁的孩子，就是世界第一黑客，声称拥有键盘就可以对世界构成威胁的黑客帝国领军人物——凯文·米特尼克（Kevin David Mitnick）。

❶ 世界第一黑客凯文·米特尼克

凯文1964年出生于美国洛杉矶，父母的离异使他从小就沉默寡言、孤僻倔强。小学时，家里那架老旧的电话是他独坐家中时唯一的游戏工具。一根电线和几块塑料便可以把声音远远地传送出去，这让他觉得极为神秘和有趣，于是他自然疯狂地迷上了无线电，并在很短的时间内成为了无线电组装和改良的行家里手，甚至还搞出过几个不大不小的发明。只是在申请专利时，很多人对一个10岁孩子申请的专利感到啼笑皆非，对其可靠性和实用性深感怀疑，甚至连专利申请表也没有耐心看完。这个不算小的打击，让凯文产生了严重藐视权威的想法。第一批计算机出现之后，其强大的功能让凯文深深沉醉于其中不能自拔，当他得知计算机可以用程序进行控制和二次开发时，便对他的第一任计算机老师说：“我想这将成为我的第三只手。”

“三只手”在中文中有特定的含义，凯文想象不到，在不久的将来，这个“第三只手”真的让他名震江湖。

逻辑思维能力很强的凯文，对计算机语言的研究和学习可谓废寝忘食，他编写的程序简洁明了，甚至令他的老师也深深折服。他常常一个人

在学校的计算机室鼓捣到深夜，害得妈妈不得不顶着月色来学校给他送夜宵，后来她索性拿出积蓄给他买了一台在当时看来性能非常不错的计算机供他使用。从此之后，就很少能在教室里看到凯文的身影，而更多的时候，他全身心地投入到计算机那美妙神奇的世界里流连忘返。

20世纪70年代中期，美国已经开始有了小规模的社区电脑网络，凯文当然在第一时间交付了网络费用。在凯文所在的小区里，电脑网络可以连接到附近的一所大学，并由大学的交换机连接到美国各地，虽然中转连接速度慢得惊人，但这已经让凯文惊喜不已了。

一个无意的机会，他连接到了北美防空司令部[①]的主页面。所有男孩子对武器都有一种天然的喜爱，几天之后，痴迷于其中的凯文便不甘心只浏览一些普通的页面，他发现在这些可供大众浏览的页面背后有着一些只有凭借密码才能进入的页面，那小小的脑子里自然产生了想看一看的念头。

他开始尝试连接到这个神秘网站的后台页面，简单的暴力破解密码无效后，他开始与一个同学合伙尝试用编程的方法进行自动破解。工夫不负有心人，15岁的凯文在经历了一个多月的试验之后终于打开了第一层密码页面，然后按图索骥，开始尝试进入北美防空司令部核心网络的计算机主机，在不长的时间内就把那块不大的硬盘翻了个底朝天。

两个月后，他悄无声息地退了出来。“那里面再没什么值得我留恋的了。”但那里面到底有些什么呢？一些与之相交甚密的玩伴们有时候会悄悄地问他。

“我知道美国所有指向俄国及其盟国的核弹头数量和分布。”扬扬得意的凯文会偶尔打开计算机，向那些和他一样大的却还只知道玩“老兵抓贼”的玩伴们展示自己的成果。那些半大的小子们在看到了计算机屏幕后，终于彻底地折服了，很自然，他们怀着崇敬的心情把自己的所见所闻

① 北美防空司令部，North American Air Defense Command，简称“NORAD”，位于美国科罗拉多州夏延山下的混凝土工事当中。

和凯文的创举讲给周围的人听。于是，凯文不仅仅在那个社区出了名，甚至得到了美国国防部官员的亲切接见。

“这的确是一个堪称经典的行动，一个15岁的孩子窥视国家机密防务信息竟如探囊取物，简直令人恐怖。”美国国防部如此评价，“如果他不是只出于游戏和好奇心理，他得到的这些数据足可以让俄国人出价几百万美元，而我们如果重新布置防御系统的话，其花费将高达数亿美元。”

对于美国军方来说，这无疑是一记超重量级的耳光，五角大楼对此十几年一直保持沉默。1983年，好莱坞以凯文的故事为蓝本拍摄了一部名为《战争游戏》的电影，影片中小主人公的所作所为几乎引发了第三次世界大战。当然在电影里是以小主人公的最终失败为结局的，但真想让这个天不怕地不怕的毛头小子承认失败，似乎是一件非常难以办到的事情。

闯进北美防空司令部的胜利带给凯文的刺激和与同龄人相比的优越感，自然超过了国防部询问时的冷脸。凯文信心大增，热情高涨。诺基亚、花旗银行、北联信息服务中心，甚至五角大楼的中央数据局和全美工业机密电脑中枢等重要部门，都成了他闲庭信步的好去处。他来去自由，在那些密级极高的军事和商业信息流中翩然来去，如入无人之境。

一次次的征服和随之而来的快感，让凯文对更高一级的挑战跃跃欲试。家里留给他印象最深的就是那部老式的电话机，一根电线可以将声音传递到世界各地，这无疑对一个15岁的孩子来说有着无比的新奇感。于是他选中了下一个进攻目标——太平洋电话公司。

没想到破译一家电话公司的超级用户密码要比北美防空司令部轻松得多。几天下来，凯文便可以随意出入太平洋电话公司的主机，得到了总统和一些明星的保密电话并用街头电话无数次骚扰，常常把这些明星和国家重要人物半夜里惊醒，然后告诉他们“打错了”，令这些金字塔最顶层的人物哭笑不得。太平洋电话公司也不得不连连道歉，随后便意识到是有人破解了公司的用户密码，而他们所采取的改进措施是不断地改变密码内容，但遗憾的是，这对于凯文来说不过是小菜一碟。

在入侵太平洋电话公司的同时，凯文对那种无绳且可以随身携带的移动电话自然也产生了非常浓厚的兴趣。当时无论从规模到技术含量，摩托罗拉公司都堪称业界顶尖，而MicroTAC系列移动电话正是摩托罗拉公司的当家产品。凯文对这种电话的兴趣除了它可以无线通话外，外形上更接近于自己经常玩的名为“星际迷航[①]”的电脑游戏中的太空人的通话器，这让凯文觉得很有必要搞清楚这种塑料外壳包裹下的工作原理。于是，在数次试探性的攻击之后，凯文便大张旗鼓地开始对摩托罗拉下手了。说来奇怪，摩托罗拉公司的中央电脑系统在凯文的敲门砖下纹丝不动，固若金汤，电脑最高管理员的密码和后台程序也似乎用一种很先进的程序进行了高质量的加密处理。这让他兴趣大增，越严密的系统对这个兴致盎然的孩子来说就越有挑战性，而越具有难度的挑战越能满足他的好奇和对胜利的向往。

正巧，有位漂亮的邻居女士正是这家移动电话公司中央服务器的工作人员。通过这位女士的“热心帮忙”，他对那套被称作“SecurID保护”的加密程序核心算法有了一些必要的了解。随之而来，这个对计算机程序有着极强天赋的少年，专门针对这种保护系统自行开发了一套行之有效的破解程序，并很巧妙地植入到摩托罗拉的电脑中央服务器中。于是在某位拥有较高权限的业务经理敲入自己的用户名和密码之后，那套被凯文植入的跟踪程序很忠诚地执行了窃取密码指令，随后凯文便用那位业务经理的密码打开了摩托罗拉的“大门”。

在掌握了这位业务经理的密码之后，为了稳妥起见，凯文并没有将其密码修改，而是专门制作了一套回馈程序并绑定在这个已经到手的用户名和密码上。只要用户更改了自己的密码，系统将在第一时间将新密码返回到凯文的手上，这样就不会引起人们的注意。因为不修改密码，业务经理就不会发觉自己的密码被盗，凯文便可以安全地在这里扎根，尽可能长时

① 星际迷航，“Star Trek”，美国著名科幻电视连续剧。

间地潜伏在这里得到他感兴趣的东西。

通过这个工作积极的业务经理，凯文很快就破译了更高级别的用户名和密码，由此他可以随意远程访问摩托罗拉的内部服务器，并陆续找到了有关MicroTAC系列移动电话工作程序的源代码。当时的凯文目的很单纯，除了锻炼自己的破解技术，顺便了解一下移动电话的工作原理之外，没有为了金钱而将到手的源代码出售给其他一些相关的公司。在发现自己被摩托罗拉公司的网络监控系统发现之后，他及时地清除了遗留在系统中的各种痕迹，悄无声息地退了出来。

这一天，凯文百无聊赖地翻看着太平洋电话公司的内部资料，无意间点击进入了FBI的主页面，一张张犯罪分子和间谍的机密材料让他非常感兴趣。于是他轻而易举地破解了后台管理员密码，成功地进入了调查局的主机。然而令他大吃一惊的是，里面居然有一份“太平洋电话公司申请调查的人员名单”，打开一看，第一页上便是一个“据初步调查，年龄20左右、家住××社区附近的男性学生”这样一条线索。虽然没有真正追查到自己头上，但通过他在街边打的那些骚扰电话的地点和通话录音等判断，这些极有可能与他画上等号。

这个发现令凯文浑身一震，脑子里又浮现了国防部调查人员面对着他时那张不苟言笑、冷冰冰的面孔来。

❷ 入侵的艺术

凯文在FBI的页面上发现了很多高级特工正在将调查的方向转向自己时，他吓出了一身冷汗。

所幸对于“20岁左右”、“大概家住××社区”之类笼统得几乎毫无明显特点可言的信息，凯文还不至于落荒而逃。这个15岁的孩子立即施展浑身解数，用了两天时间找到了FBI中央处理系统的电脑密码，然后进入

了FBI的中央数据库，一边嘲笑这些所谓无所不知、无所不能的高级特工的无能和笨拙，一边恶作剧地将几个负责调查凯文事件的特工的个人档案调出来，将他们的照片全部搬到几个臭名昭著的罪犯档案中。

多次的战无不胜使得凯文这一次居然忘了“反侦查”，他在FBI主机里所做的一切，被特工们早些时候植入的跟踪程序记录下来并顺藤摸瓜找到了他的住所，第二天就将凯文堵在了家里。

一个稚气未脱、实际年龄不到16周岁的孩子居然将FBI的中央电脑系统视做自己为所欲为的游乐场，这不能不让那些自称“在电脑最尖端领域里摸爬滚打了多年”的资深探员们汗颜。惺惺相惜的感觉油然而生，况且16岁不足处以刑事处罚，加上当时的联邦法律对于高科技犯罪还没有明确的处罚规定，很多青少年保护组织也对这位计算机界的天才儿童鼎力相助。凯文在造成了巨大的社会影响和经济损失之后并没有被深加追责，当局只是将他关进了管教所，这也使凯文成为世界上第一个因电脑高科技犯罪而被实施批捕的罪犯。

两个月后，凯文恢复了自由，但电脑带给他的无形刺激和胜利的诱惑并未让他就此罢手，反而促使他急不可耐地一头扎进了电脑网络之中。短短的时间内，他先后入侵了多家商务网站和国际大公司，无端毁坏重要数据，向无关人士发送错误的订单和催款单，搞得这些大公司疲于道歉和赔款，而人们第一个怀疑的自然就是这个曾经轰动一时的小黑客。在掌握了大量的证据之后，当凯文将手大胆地伸向美国轻工业联盟的集中管理系统时，再一次将他人赃俱获。

这一次他就没有第一次那样幸运了。当局指控他在网络上窃取了价值140万美元的软件，并造成多家网站高达数百万美元的损失，甚至连他要求假释的请求都被法庭拒绝。凯文在网络上如入无人之境的高超技术和造成的巨大危害，使得当局认为他只要拥有键盘就会对社会造成威胁，因此凯文被判一年徒刑并处以巨额罚款。

出狱后的凯文没有学校和雇主愿意接收他，而当初的巨额罚款又让凯

文不得不尽快找到一份高薪的工作。在多次碰壁后，他不得不继续从事黑客活动，并将一些到手的机密文件高价卖出以偿还因罚款而欠下的债。直到1983年，FBI在接到多起黑客骚扰投诉之后重新将目光锁定了凯文，但凯文显然是“吃一堑，长一智”，入侵后他会利用自己高超的电脑技术将留下的痕迹处理得干干净净，使得FBI想尽了一切办法也没有找到他犯罪的证据。这些智商与凯文相比明显偏低的特工们想到了一个最笨的办法：让一个小有名气的电脑黑客来卧底，诱使凯文与他合伙入侵一个高保密网站。

在这方面，凯文是不需要太多条件的，黑客的刺激和入侵成功后高额的回报让他几乎未经思考便一口答应。但凯文的细致在于他自从出狱后便时时关注FBI的内部动向，而这一点，凯文在进入调查局的网站后自然会一清二楚。在他与黑客第一次尝试入侵失败后，他便在调查局的网站上发现了卧底黑客向调查局提供线报的情况，立即明白自己中计了，于是当天夜里凯文便神奇地消失了。FBI以那个卧底黑客的线报为依据，向法院申请正式的刑事通缉令。

逃亡中，凯文不断地往家里汇款，用以继续偿还债务，而他的收入来源自然是利用自己的黑客技术。1994年年末，凯文向圣迭戈超级计算机中心发起了一次冲击并成功得手，获得了较高回报，这一次攻击被载入了史册，被称作“第一次真正意义上将计算机网络置于高危险境地”。而正是这一次堪称典范的攻击，却惹怒了另一位计算机专家——日本人下村勉，一场龙争虎斗即将开始。

❸ 被FBI通缉的日子

下村勉是个日本籍的计算机专家，圣迭戈加利福尼亚大学（UCSD）超级计算中心的主席特别研究员，因其在计算机网络安全方面的卓越贡

献，被冠以“世界第一安全专家”。这是一个计算机安全第一专家与计算机入侵第一高手之间的矛与盾较量。

下村勉受聘于圣迭戈超级计算机中心，负责中央服务器的网络安全工作，对于这个早已名声在外、年龄不大，但手段高超的黑客从自己手中不费吹灰之力便窃取了众多的情报，“我这个全美最专业、最出色的安全专家栽到一个不到30岁的小伙子手里，这是个严重的耻辱。”下村勉感觉极丢脸面，立即向FBI请缨，愿意无偿协助美国国家安全部门将凯文绳之以法。

得到了下村勉的帮助，FBI更是如虎添翼，在世界范围内对凯文进行通缉。而一向高傲自信的凯文对于警方的追捕能力不屑一顾，一边通过计算机网络了解警方的动向，一边饶有兴致地给下村勉发了一封“顺致问候”的电子邮件。在信中，凯文用最彻底的嘲笑口吻向这个全美计算机第一人发出挑战：“说实话很早以前便得知先生大名，但我一直害怕自己的技术不过硬，上帝安排我们在这一事件中一决高下，而现在的我经过若干次的历练，对自己的技术有了足够的自信，相反却对您创立的计算机安全技术理论和实践活动抱有最彻底的怀疑。在我面前，它约等于一张脆弱不堪的打印纸，你相信一张打印纸的保护厚度可以阻挡我的脚步吗？我们开始吧，让世界瞩目这场较量，相信以我的能力，会是一个很相称的对手，即使我不能获胜，但全身而退绝对不是问题，你和你所协助的愚蠢的FBI在我身上将一无所获，而我将继续畅游世界的梦想和历程。”

目空一切的凯文没有想到的是，仅仅凭借着这封电子邮件，机敏警觉的下村勉便找到了蛛丝马迹。虽然凯文在发出这封邮件的同时对自己的IP地址等信息进行了转移处理，但还是被有着独到反黑客技术的下村勉找出了破绽。在接下来的一个月的时间里，下村勉抛开了手中的一切琐碎事务全力追查凯文的下落，通过自己多年对计算机网络安全领域新技术的探索，他凭借一系列的先进技术手段对凯文的藏身之地展开追踪，并成功地将追踪范围逐步缩小。与此同时，凯文也在夜以继日地实施着反跟踪，他

不断地布下迷阵，将自己的行迹隐藏起来，同时不断地通过转移IP地址等手段给自己的对手制造假象。当下村勉的计算机追踪程序发现凯文在佛罗里达时，凯文其实正躲在阿拉斯加的火炉旁喝他钟爱的蒙古马奶酒。为了证实自己不是个缩头乌龟而是个货真价实的超级黑客，凯文不断地给下村勉发送信息，并故意留下飘忽不定的足迹供对手追踪，诱使下村勉上当，他甚至请自己黑客圈中的朋友在千里之外冒用自己的信箱和口吻给下村勉发信，教那些在他眼中技术水平尚显稚嫩的黑客朋友怎样隐藏真实通信地址，并且不露痕迹地暴露一个假的地址信息。在一连串措辞狂妄的信件中，他小心翼翼地留下些虚假的破绽给下村勉制造困难和技术难题。同时他不断地冲击下村勉的计算机系统，试图捣毁对手的追踪体系或者是得到追踪方法，当然，他更希望破获下村勉的追踪源代码并将之公布于众，从而一举确立自己第一黑客的地位。

在反黑客领域中，经验丰富、技术全面的下村勉识破诡计，他抽丝剥茧般逐层剔除凯文制造的让他感觉头疼的虚假信息，从中找出真正让他有所收获的有用数据加以整合和分析，同时在与凯文的计算机互相攻击过程中不断加大追踪力度和改进自己的程序。他惊讶地发现，自己这个平生仅遇的对手虽然只是一个年纪轻轻的毛头小子，但他技术全面、头脑冷静、分析透彻而且具备了极高深的计算机网络技术，这令他斗志昂扬。在与凯文你来我往的多次周旋之中，下村勉一直致力的反黑客技术体系也不断完善。当初他在编制反黑客系统的时候因为没有真正高水平的对抗机会，只是凭借着自己一厢情愿的想象制定和完善这一体系，自从凯文出现之后，层出不穷的黑客攻击手段让下村勉在真正意义上弄懂了尖端的黑客攻击技术，大开眼界的同时，无形中使他的研究成果丰富和完备起来。“我不得不感谢你为我做出的这一切，它使得我的网络安全系统脱离了纸上谈兵的阶段并最终成为一种实用可行的体系。无论谁输谁赢，从这个角度上来说你对我帮助极大，甚至是个功臣，或者可以设想，无论最终结果怎样，我想我们可以很平和友好地喝上一杯。”在他给凯文的一封回信中他如上述

写道。而不可一世的凯文则措辞强硬，“老子仍然是天下第一，能仅凭技术手段而不是手枪抓到我的人，时至今日仍然没有出现，你这个自称天下第一的计算机安全专家，不过是浪得虚名而已，同样对我无能为力。”

为了不给下村勉太多机会，凯文有时候会使用经他改制过的调制解调器，连接某些公用电话交换中心来与他的黑客朋友们联系，同时他在一个极其隐蔽的BBS上开辟了一个需要密码才可进入的空间来同朋友们取得联系，这反倒给了下村勉一个追踪他的可乘之机。经过了缜密的分析判断之后，下村勉终于可以肯定的将凯文的行踪报告给FBI了，他通过那条接入了北卡来罗纳州公用电话系统的数据报告单，查到了一个地点固定但IP地址自动更换的飘忽不定的信号源，而一般网络用户的IP地址段在同一固定地点是不会有极大波动的，可以肯定这个接入源应该是个有着特殊目的的网络客户。这个可以自动更换IP地址的信号源，其实正是发自凯文自行改制后的调制解调器。

4 梦断情人节

1995年的情人节就要到了，漫天大雪丝毫没有影响到恋人们表达自己爱意的心情，花店的生意十分火爆，街上到处弥漫着鲜花的清香和爱情的缠绵气息。下村勉与身着便衣的FBI探员把车停在北卡来罗纳州罗利市的一条狭窄的小巷里，穿过成双成对相拥而过的恋人们组成的爱情队伍，来到一片破旧低矮的贫民窟。

“这倒真是个绝好的藏身之所。”下村勉为凯文独到的眼光折服，一边抖落着肩上的雪花一边由衷地赞叹。FBI的探员们却没有任何欣赏景致的心情，这个法力高深的年轻人把这些自命不凡的探员们折磨得简直苦不堪言，好不容易找到了这个捣蛋鬼的藏身之所，他们自然不会掉以轻心。

经过两天的不间断监视，探员们终于锁定了凯文的住所，在联系了当

地的警察局之后，一张大网悄然张开。鉴于凯文是个极度危险而狡猾的人物，而且善于销毁罪证，下村勉建议不轻易惊扰这个天才黑客，而是在掌握了凯文的活动规律之后再进一步行动。在一个阴冷的清晨，当凯文穿着臃肿的棉大衣出门之后，下村勉进入了凯文的家。

简陋的房间阴暗潮湿，这种艰苦的环境很难与一个手中经常掌握着数以百万美元计的重要资料的黑客联系在一起，不过下村勉显然不是来对那些零乱的家居品头论足的，他的兴趣在于桌上凯文没有带走的计算机。打开电脑之后，下村勉惊喜地发现这个极端自负的超级黑客自己的计算机居然没有任何密码，也许凯文认为天底下真的不会有人注意到自己躲在这样一个隐秘的角落里。“没有一个人能找到天才的凯文”，他不是一贯这样说吗？一时疏忽的凯文也没有及时地对自己的计算机进行使用记录的清理，这让下村勉大喜过望，在仔细地翻阅了凯文的使用记录并掌握了相关的证据之后，下村勉对其进行了拷贝，这将是起诉凯文的最直接证据。

当吃过早饭、满面红光的凯文重新回到自己的家门口时，两个FBI探员一左一右夹住了他。“小子，你害得我们圣诞节和情人节都在陪你周游世界，你知道吗？”

凯文的第一反应是微微一笑，然后，他便凭直觉在人群中找到了下村勉的目光，“那精明强干的目光里透着坚韧和些许的愤怒，我知道他一定就是与我较量多日的下村勉。不过我要说，我只需在离家之前花费两分钟时间对电脑进行清理，你们还是奈何不了我，我输在了大意，从而成就了下村勉。当然，我要保持我第一黑客的风度，我承认单纯地从技术来说，我还是输了。”凯文这样回忆。

随之而来的审讯中，凯文态度良好，风度依然。他谈笑风生，那些存储着最高级别国家机密的计算机防御体系对他来说，是“形同虚设，脆弱得不堪一击”。而对于出庭作证的下村勉，他则显得很有礼貌，并恰如其分地表示了自己的尊重和佩服。“你很棒，我钦佩你的技术，你是第一流的计算机安全专家。”

美国法庭对凯文的所作所为感到吃惊和心有余悸，法庭宣判拒绝他以任何形式获得假释和保释，他们坚决地认为凯文如果有着自由的身体和行为，“整个世界都会乱套，全球的所有信息都根本没有安全可言。”一些凯文“光顾过”的公司也联名要求对这个世界级的危险分子重罚重判。“我们对是否限制他的自由不感兴趣，只要他不再接触电脑和互联网，我们就谢天谢地了。”很多拥有着保密级别很高的信息部门这样感叹，“种种实践证明，任何高超的信息保密技术在凯文眼里都如若无物，这让他们胆战心惊。”

很不幸，凯文将在狱中待上很长一段时间，而习惯于颠沛流离的凯文，对这种可以相对安逸和放松的生活也有些向往。在自己的单人牢房里，他把房间收拾得一尘不染、井井有条，每天做操训练，甚至饶有兴致地把十根手指按在墙上，在一块无形的键盘上编写自己的计算机程序，这举动让那些看护他的狱警们瞠目结舌。日子久了，凯文便有些烦躁不安，毕竟那块无中生有的键盘不可能满足他强烈的操作欲望，而长时间不能入侵高难度信息中心的刺激让他感到空虚和失落。在十几年的黑客生涯中，他一直受到业界众星捧月般的顶礼膜拜，这一切荣耀和光环消失之后，他因为失落而开始变得沉默寡言，这让那些来探望他的黑客朋友们大失所望。

两年之后的1997年，世界最著名的Yahoo网站被一群不明身份的黑客袭击，并声称如果当局不释放凯文，“全美国甚至全世界都将失去一个不可多得的计算机天才。鉴于此，我们在很久以前便在这里埋下了逻辑炸弹，如果当局不满足我们的愿望，过去一个月中浏览过Yahoo网页的计算机用户都将受到严重的损失，我们的最后期限是1998年圣诞节，如果当局不给我们一个满意的答复，这些逻辑炸弹将被非常准时地引爆，美国当局会因为错误和固执地囚禁凯文而成为世界的罪人。一旦凯文获得自由，我们将重新在Yahoo网页上植入破解程序，让那些逻辑炸弹失效。”更早以

前，众多黑客组织也声称，如果当局继续虐待一个对计算机发展进程有着杰出贡献的、世界级的电脑领袖，他们将启动已经植入到网络中的计算机病毒，“像世界毁了凯文一样毁了这个世界。”

一个30多岁的黑客，竟拥有如此的声望和地位，这让当局很是难堪，也让百无聊赖、无所事事的凯文多少感觉到一丝欣慰。

2000年1月，凯文获释，当记者采访这个黑客世界的风云人物，并询问他今后有什么打算时，凯文仍然念念不忘他钟爱一生的计算机。“我的计算机技术几乎都是在实践中自己摸索出来的，我想如果可能的话，准备先上大学，系统地学习计算机知识。”

当然了，这很有难度，只要凯文的手按在键盘上，整个计算机世界都似乎被扒光了衣服一样毫无秘密可言，法院在得到当局认可之后，迫使刚刚换了新衣服准备走出监狱的凯文在一张保证书上签字，要他保证在无人监护的情况下不得擅自使用手机、计算机、调制解调器等与信息相关的电子设备，更不准私自接入互联网，他只能通过信件的方式与朋友联系。

“那我出不出来，好像就没什么特别的意义了。”凯文一脸的无可奈何。

现在的凯文虽然风云不再，但依然声名显赫，世界上几乎每一个与计算机有过接触的人都知道这个大名鼎鼎的人物，略微发福的凯文后来成为了一名计算机信息安全领域的公众人物和领军人物，并在政府的严格监督下运营着一家网络安全公司。在政府的批准下，很多保密级别很高的网络公司甚至美国国家安全部门雇佣他入侵自己的系统，发现他们的安全问题，并在被那些图谋不轨的家伙发现之前打上补丁。

刀之双刃，既能伤己又能伤人。凯文作为计算机发展史上第一个，也是成绩最突出的优秀学生，在世界级的考验中屡屡过关，独占鳌头。改过自新的他，也正凭借着高超的计算机技术，在这个高手林立的电脑世界里，续写着一个美丽得近乎恐怖的神话。

【黑客知识】

下村勉：1964年生。日裔美籍电脑安全专家、计算物理学家，是化学家下村脩的儿子。子承父志，因与和他同龄的超级黑客米特尼克的巅峰对决而一战成名，成为当今世界上最优秀的计算机安全专家。

他出生于日本，在美国新泽西州普林斯顿长大。高中时破格进入加州理工学院就读。大学毕业之后，进入美国洛斯阿拉莫斯国家实验室工作。现为圣迭戈加利福尼亚大学（UCSD）超级计算中心的主席特别研究员。

IP地址：全球每个电话都有一个唯一的号码，以区分用户，换句话说，电话用户是靠电话号码来识别的。同理，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP地址”。IP地址的作用等同于家庭住址，在所有接入网络的计算机中，不可能有重复的IP地址。IP地址是一串数字，三位一组，共四组，前几组用于标明计算机用户的地理位置，最后一组则随机分配，技术人员通过分析前几组数字便可以推算出一台计算机用户的大概地理位置。曾经有人通过技术手段给国内常用的QQ软件加装了“显IP”功能，其功能原理便是通过分析用户的IP地址来显示其所在城市的地理位置，其精确度甚至可以显示出某个用户在哪个网吧上网。而一些不想把自己的IP地址公布于众的人，也会通过一些代理网站和编写代码等方式改变自身的实际IP地址，用一个虚假的IP地址掩盖自己所处的位置以混淆他人的视线。这也是凯文与下村勉捉迷藏的惯用方式之一。

附：来自凯文·米特尼克的忠告。

（1）备份资料。记住，你的系统永远不会是无懈可击的，灾难性的数据损失会发生在你身上。

（2）选择很难猜的密码。不要没有脑子地填上几个与你有关的数字，在任何情况下，每隔一段时间都要及时修改自己的密码。

（3）安装计算机防病毒软件，并让它每天更新升级。

（4）及时更新计算机操作系统，时刻留意软件制造商发布的各种补丁，并及时

安装应用。

（5）在IE或其他浏览器中会出现一些黑客鱼饵，对此要保持清醒，拒绝点击，同时将电子邮件客户端的自动脚本功能关闭。

（6）在发送敏感邮件时使用加密软件，也可用加密软件保护你硬盘上的数据。

（7）安装一个或几个反间谍程序，并且要经常运行检查。

（8）使用个人防火墙并正确设置它，阻止其他不明的计算机、网络和网址与你的计算机建立连接，指定哪些程序可以自动连接到网络。

（9）关闭所有你不使用的系统服务，特别是那些可以让别人远程控制你计算机的服务，如RemoteDesktop、RealVNC和NetBIOS等。

（10）保证无线连接的安全。在家里，可以使用无线保护接入WPA和至少20个字符的密码。正确设置你的笔记本电脑，不要加入任何网络，除非它使用WPA。要想在一个充满敌意的网络世界里保护自己，的确是一件不容易的事。你要时刻想着，在地球另一端的某个角落里，一个或一些毫无道德的人正在刺探你的系统漏洞，并利用它们窃取你最敏感的秘密，你很可能会成为这些网络入侵者的下一个牺牲品。

—— 第九章 ——

打开潘多拉的魔盒，探寻黑客犯罪之路

探寻黑客犯罪之路看似最安全的位置恰恰最薄弱。插好网线，按下电源，世界将呈现最彻底的坦诚，它可以告诉我们想要的一切秘密。

——约翰·李

❶ “发疯”的ATM取款机

黑客，自从这一职业诞生之日起，就不可避免地与金钱挂上了钩。毕竟，钱可以说是一切行为的原动力，只有钱才能对人的主观意念、对人的思维和行为起到最直接的指导意义，甚至可以说，钱是一切犯罪的根源之一。

在著名影星施瓦辛格主演的电影《终结者》中，小主人公约翰·康纳把一张作废的磁卡连接到ATM机上，然后打开了自己的笔记本电脑，启动了某个程序，按下几个按键后，ATM机便吐出了三张百元大钞。这个镜头虽然只有短短的几十秒，但无疑却是每个黑客都曾做过的梦。

在2010年黑帽大会上，来自西雅图IOActive公司安全测试总监巴纳比·杰克（Barnaby Jack）的表演让所有到会的人重温了这一幕，他的演讲和示范内容，居然是现场破解ATM取款机。

ATM机是世界通用的自动提款设备，一张磁卡，几个数字密码，就可以让一台冰冷的机器吞吐出无数的钞票。但机器提供的这种方便快捷的存取方式，无疑也成了正义和邪恶的角力场，银行方面会时时就其设备的安全性进行更新，而一些心怀不轨的人，则把目光贪婪地瞄向了这种会吐钞票的机器。时至今日，还没有人成功地从ATM机上盗取现金的记录，这让银行系统对这种机器的安全性充满了信心，但杰克的演示无疑给自信的银行敲响了警钟。

澳大利亚籍，现居住圣荷西的网络安全专家杰克在黑帽大会上演讲时声称，“有些装置从外表上来看固若金汤，但我希望改变大众对这些装置的看法。”他把两台ATM机搬到现场，轻轻按下几个按钮，ATM机便发疯一般自动吐出一堆钞票。“我只是想说，很多东西不是真的拿他们没办法，只是很少有人敢这样做。就像米特尼克攻陷美国航天局之前，人们都认为那里是最安全、最可靠的一样，而一旦它的金刚不坏之身被打破，就像打开潘多拉的魔盒一般，整个世界都为之改变了。”

在随后的讲解中，杰克声称现场的这两台ATM提款机与市面上的普通提款机完全一样，分别由Tranax Technologies和Triton公司制作，只不过杰克在过去几个月的研究中发现了一项安全漏洞可让黑客通过电话机连上ATM机，并可以在不知道密码的情况下向ATM机发出取款指令，而这台看似聪明的机器则会认为卡号与密码是对应的，也就会立即吐出全部的现钞。

他说：“我见过的每一台ATM机，都可以找出安全漏洞，黑客能轻松让机器吐出钞票。我监测过四台ATM机，四台都一样。”杰克的表演引起一片哗然，黑帽大会尚未结束，这两家ATM机的制造商就第一时间与杰克取得了联系，随后立即更新了软件设计，堵住了安全漏洞。

所谓哪里有钱，哪里就有犯罪，老话自有其道理。黑客时代，如果要修改这句话，不妨说：“哪里有钱，哪里就有黑客。”

在杰克之前，所有针对ATM机的盗取现金行为都不过是小打小闹。

一些人私接外挂程序，绕过ATM机的识别组件，ATM机以为它们吐的是1美元美钞，但实际吐出的是20美元；另外还有一些专门针对ATM机研制恶意程序可以欺骗ATM机的中心识别程序，如TSPY_SKIMER 恶意程序系列就是专门攻击 ATM 提款机的。这些程序虽然功能强大，但必须手动植入到提款机的主板芯片中，而所有对ATM机的改动，银行只需要安装一台视频监视器，同时加装一个系统组件运行报警器就足够了。在吐出钞票之前，系统会检查所有组件是否有一次成功且完整的运行，若是发现某个组件被绕过，没有运行，系统会拒绝付钞。

目前大多数ATM机采用Windows CE操作系统与ARM处理器，通过一个串列接口（serial port）连接来控制钞票箱的存取动作。杰克指出，他用标准的“除错”（debugging）技巧中断正常的开机程序，在Tranax生产的ATM机中找到一个远端存取的安全漏洞，让他无须密码就能远程入侵ATM机。

至于Triton生产的ATM机，他未发现明显的远程存取安全漏洞，不过他发现吐钞的主机芯片只靠一把标准的密码钥匙保护，在网上10美元就可以购买一片。他还发现，在复制了密码保护芯片之后，他可以强迫这种品牌的ATM机无条件接受他远程植入的软件，并把这套软件当作合法的软件重新写入系统主板。一旦植入这种程序，杰克就可以随时用一套组合密码向ATM机发出吐钞命令，“而这乖巧的机器再不会拒绝我的邀请。”

杰克原计划在黑客大会上发表类似的演讲，但由于在黑帽大会上的表演引起了银行业的震惊，许多银行一致反对杰克在任何公开场合表演，以免引起更大范围的恐慌和给黑客们跃跃欲试的理由和技术教唆，杰克所在的Juniper Networks公司严令阻止了杰克继续出风头。

虽然杰克在第一次演讲的一开始，就宣称自己不会发布任何破解ATM机的公用程序和具体破解思路，但他的这一举动无疑激起了黑客们入侵ATM机的信心。因此杰克甚至被视作银行界的头号公敌，黑帽大会还未结束，就不得不收拾行李回他的办公室，而他的银行卡也受到了银行

的密切关注，每一笔存取都要得到多方确认才被认定为有效。

为此，杰克不无遗憾地说，“他们怕我的表演让他们信用扫地，而我不过是敲了下警钟而已，如果你们真的认为我是害群之马，那么当未来的某一天，一个神通广大的黑客真的用一张废弃的银行卡掏空了ATM机，真正丢面子的应该不会是我。不过从此我真的不再相信银行了，有钱不如放在我家的壁橱里，可能会更安全也更快捷，因为我要想用银行卡取一张20美元的钞票，大概要盖十五个印章。”

❷ 银行大门挡不住的黑客

20世纪90年代的俄罗斯，经济起伏跌宕让每个人都感觉岌岌可危，随时可能降临的失业危机和每年超过40%的失业率，使得很多原本生活得很好的俄罗斯人一夜之间就变得一文不值，甚至连个面包都买不起。

贫穷的代价常常就是最彻底的反抗和自我救赎。

据不完全统计，在这场长达十年之久的经济大衰退中，有近30%的计算机从业人员转为商业和军事黑客，他们凭借自己高深的计算机技术，把目光瞄向了那些有着巨大经济价值的商业和军事目标，甚至从事双料间谍，把A的资料卖给B，再把B的资料拿回来转卖给A，如此倒买倒卖，很轻松地就可以一夜暴富。

弗拉基米尔·莱文就是其中最优秀的黑客之一。

俄罗斯人天生具有探索和求新的精神，这成就了俄罗斯人在高精尖技术领域的众多精英级人物，包括计算机领域。个人电脑在它兴起的最初年代里就受到俄罗斯人的疯狂追捧，以至于在随后的几十年时间里，俄罗斯有着世界一流的软件业和硬件业，其航天航空、电子、重型工业以及军事领域中应用到的最尖端技术人员都依靠电脑成就了非凡的业绩。但相比之下，这些高精尖的从业人员工资待遇较低，个人养老医疗都得不到很好

的保障，“买一套微软的Windows系统需要用去我们两个月的薪水，而我们只需要花上半个月的工资去买一台光盘刻录机，就可以制造出无数的Windows，这对任何人都是巨大的诱惑。”而贩卖盗版软件似乎只是小儿科的事情，那些精英级的人物是不屑为之，比如弗拉基米尔·莱文，他的目光看到的是那些放在银行重重深门之后的一沓沓钞票。

莱文与大多数黑客一样，是泡黑客论坛成长起来的。自小喜好数学和逻辑学的莱文天生对计算机有着浓厚的兴趣，在一些黑客论坛里摸爬滚打了几年之后，莱文俨然已经成为领袖群伦的重量级人物。随着美国大兵进驻科索沃地区，俄罗斯激进派人士大力抨击美国的霸权行为，在这种政治环境下，那些热血黑客们往往充当了排头兵。莱文在俄罗斯经济的不景气中失业后，也萌生了攻击美国银行的想法，而在黑客论坛里掌握的计算机和网络知识则给他提供了强有力的技术支持。

1994年，刚从圣彼得堡科技大学毕业的莱文工作仅仅三个月后就失业了，整天无所事事地游荡在各大黑客论坛里，当看到有个帖子声称美国花旗银行的网上支付系统似乎经常出现系统崩溃的现象之后，他敏锐地感觉到这应该是银行网络系统的缺陷造成的。对于黑客而言，系统缺陷就暗示着可以找到进入的“跳板”，而一旦成功进入银行网上支付系统的后台管理页面，便可以对储户的个人信息，包括密码都一览无余。

这发现让莱文异常兴奋，在那个帖子后面他貌似无心地跟了帖，具体询问了花旗银行系统崩溃的发作规律，然后与三五个同样泡在黑客论坛的朋友决定一试身手。

经过多次试探性地在花旗银行的网上支付系统上访问，莱文发现每当系统进行到“点击确定按钮进行付款”的时候，系统就会反应迟钝，页面很久无法刷新，而当使用者强行关闭这个疑似崩溃的页面之后，偶尔会出现你的银行卡里的钱并没有支付而系统却认为你已经完成交易的情况。

这说明花旗银行的系统数据库在即时更新上存在着某种冗余溢出错误，使得用户在点击支付按钮后系统无法正常做出反应，或者说，在用户

点击支付按钮之后，后台数据库是开放的，并没有即时关闭。若是能在数据库开放的极短时间内成功进入数据库，就免去了寻找数据库的位置以及刺探数据库密码的过程，整个数据库的用户信息都将赤裸裸暴露在自己的眼前。

针对这一漏洞，莱文几人日以继夜地编写一个针对花旗银行这一漏洞的对接程序，并不断地把这个程序与系统对接，试图在数据库开放的瞬间挤入系统中去。经过近一周的努力，莱文终于在同伴的帮助下成功地进入了花旗银行的系统数据库。

接下来，他只需要复制用户的各种有用信息就可以了。经过筛选，莱文选中了大约十位户头上有着巨额存款，而在最近三个月里并没有动用过银行账户的用户数据。之所以选中这几个用户，理由很简单，巨额的存款可以供莱文几人肆意挪用，而长时间未动用存款，说明用户不急于使用这笔存款，因此莱文的行为不会在很短的时间里被发现，这是最重要的，他需要时间来转移这些款项，并且逃跑。

“这么干真是够刺激的！”莱文和他的同伙们喜出望外，他似乎看到了在不久的将来身家亿万的自己在塞纳河边凭栏远眺的情景。“如果我们拿光他们所有的存款，大概可以有数亿美元。想想都感觉血脉膨胀，要知道，在俄罗斯一个大学教授每个月的薪水不过才折合150美元。”

最后莱文还是放弃了全额挪用的念头，毕竟这些钱如何挥霍都是今生也花不完的，如果花不完，钱就体现不出其应有的价值。更重要的是如果有一天被捕，他很可能因此送命。在这十个备选名单中，莱文选中了一个存款额达1300万美元的用户，数据表明这个用户在过去的一年多时间里，对自己放在花旗银行里的这笔存款不闻不问。

接下来，莱文和同伙们在芬兰、荷兰、德国和以色列等国开设了银行账户，随后他的同伙们便分头进入各国，莱文则蹲守原地。待同伴们各就各位之后，按约定时间由莱文从花旗银行里将巨款分批转移到这些在各国先期开设的户头上，而他的同伙们则立即在各国的银行里把这些钱取出。

如果不是以色列的银行因意外事故暂停存取款业务，使得莱文的同伙没能立即把钱转移的话，莱文也许就真的在得手后人间蒸发了。

事发当天，以色列的某家银行因突然的系统故障被迫停止业务，莱文于是吩咐他的同伙放弃这里的款项，立即前往中立国家瑞士，但他的同伙显然对这个结果相当地不满意，并没有马上离开，准备冒险在第二天再来试一次。而凑巧花旗银行在当天晚些时候发现有一笔巨额款项被人从银行划走，银行方面于是按照惯例向户主发送了电话告之，户主当然选择了报警，并要求银行对这笔款项的去向进行追查和冻结处理。于是，当银行发现以色列的这笔款项尚未被取出时，立即加派了人手对位于以色列的这个新开户的银行户头重点监控，第二天，莱文的同伙试图再次作案，正好被守候一旁的警察逮个正着，一场惊天迷案随即水落石出。

莱文在第二天发现以色列的同伙并未按时到达瑞士，立即转乘航班马不停蹄地逃往罗马，从此隐姓埋名。

莱文由此一手炮制了世界上第一个成功的网络银行盗窃案，也把自己从一个优秀的程序员变成了隐居他乡、张皇度日的通缉犯。直到1989年，莱文在伦敦机场转机时不小心被机场候机大厅的电梯绊倒，摔断了脚踝，就医时显示的医疗记录终于把这个远遁千里之外的银行大盗绳之以法。

莱文知道自己一旦被引渡到美国很可能就此埋骨他乡，在他的律师竭尽全力周旋了两年之后，莱文仍然没能躲开美国的审判，他将在美国的监狱里待上三年之久。

这三年的时间消磨了莱文所有的激情，出狱的莱文再没有了往日的光彩，每天躲在圣彼得堡的乡下，经营着一个大棚花室，每天面对着成千上万绽放的花朵微笑。

也许从此世界上少了一个优秀的程序员，少了一个优秀的黑客，但这一切都不妨碍莱文在世界黑客史上，占有厚重的一章和浓烈的一笔。

❸ 黑手党走向互联网

时间推进到2000年，这一次让我们到意大利去看看。

意大利的黑手党与意大利的足球一样有名，而如果你还认为黑社会都是些只会打打杀杀的粗人，那你就大错特错了。

就在这年秋天，意大利黑手党精心策划了一起模拟莱文的网络银行盗窃案，他们的目标是西西里岛政府存放于西西里银行的大约1万亿里拉巨款，并且这一次他们不需要戴着墨镜端着枪，他们只需要一台电脑和雇佣几个胆大心细的计算机高手。

100万里拉的出价，足以让任何黑客流下口水，黑手党党魁安东尼奥决定在退休之前“干一个漂亮的，应该可以青史留名的大事儿”，他首先花费巨资把西西里银行的两位高级职员拉下水。这两位职员各自掌握着银行电子密匙软件的一部分，当这两部分软件合二为一时，就会自动计算出经过二次加密的存取款密码；并且这两个职员的功能还在于，单纯地取得了这笔巨款的存取密码还不行，银行系统设定在某一时间之前，任何个人和单位不得提前支取这笔款项，而这两个职员可以在某一时刻关闭真正的银行网络系统，这样黑手党只需要在银行系统被关闭的同时，用另一套同样是这两个职员提供的银行网络系统的拷贝代替真正的银行系统，这个时间锁就迎刃而解。当然了，关闭银行系统还需要这两个职员出马。

而让他们想象不到的是，有些人不是用金钱就可以打动的，这两个职员中的一个，是被警方故意安插进来的。于是，一切的精心策划都被这个小小的疏忽打得落花流水。就在安东尼奥费尽心力搜罗来的高科技精英们在电脑前做着1万亿里拉的美梦时，一张法网将他们一网打尽。

4 “诈骗高手联盟”

计算机为整个世界开启了神奇之门，在这扇门后，一些掌握着高科技的人痴迷于运用计算机技术满足自己的贪婪，与普通的犯罪不同，计算机网络作案有时不会留下任何实物证据。随着网络银行、各种电子支付系统的普及，这在方便了广大用户的同时，也引得一些掌握了计算机技术的人私欲膨胀，在网络世界中扮演着电子窃贼的角色。

最早的股票是一张张实实在在的票据，不计名不挂失，所有的买卖都要现金交易，而随着信息时代的来临，网上炒股改变了传统的炒股方式，无纸化交易以及电子商务使得人们只要面对电脑，在键盘上敲击几个按键就可以周转巨额的款项。在这个时代，钱币的流通更大程度上只是一串串数字在一个看不到的网络上跑来跑去，计算机网络的成功应用，使得电脑在经济领域大展身手的同时，围绕着电脑的经济犯罪也跟着时代的脚步日新月异，掌握着高新技术的电脑人才很容易在巨大的诱惑面前失去底线，使自己变为盗取巨额资金的电子飞贼。人们在享受高科技方便快捷的同时，也要面临资金安全的风险，这似乎也是高科技时代不可避免的矛盾。

作为世界上著名的黑客组织“诈骗高手联盟”的创始人之一，美籍华人约翰·李，12岁成为一名黑客，16岁时就可以“免费乘坐班机，把自己的房租和水电费清零”，他可以任意改变他人银行账户上的存款金额，他声称自己按五个键就可以完成一次网络盗窃。在两年之内挥霍了从美国国立银行弄到手的360万美元之后，约翰·李被捕，在法庭上他承认“坐牢很不好玩，但如果有机会，还是不能抵抗再干一次的刺激和诱惑”。

这就是网络犯罪的最普遍心理，正是这种凭借计算机技术不劳而获的“成功”，让一些人疯狂和痴迷。

金融业永远是黑客的高度集中区，也是网络犯罪的重灾区。1998年10月，三个十几岁的中学生入侵了美国一家电子产品零售店的主服务器，

窃取了八千余份在线信用卡订购单；2000年，美国一家信用卡公司的网站被攻破，存有数万个信用卡用户信息的数据库遭到洗劫，迫使这家公司不得不重新向所有用户发放最新加密的信用卡；2000年2月，英国《泰晤士报》报道，一批黑客在过去一年里至少向12家跨国公司的电脑系统发起攻击并得手，其中一家VISA信用卡公司被勒索1000万英镑，黑客在这家公司的系统中窃取了刷制信用卡芯片数据的软件程序，并声称如果该公司不合作，将使该公司的整个系统陷入瘫痪。该公司拥有近10亿个信用卡用户，一旦系统陷入瘫痪，每天的损失就将高达数千万英镑。

随着瞄准银行卡的犯罪手段日益先进，信用卡和银行系统的核心代码及防范措施也越来越完善，但不可否认，无论信用卡运用了多么高深的技术，只要它还是由程序刷制的，就同样可以被不法之徒加以复制，而这个世界上也许根本就不存在万夫莫开的安全系统，完全没有攻击漏洞的系统根本就不存在。

❺ 中国第一网上盗窃案

相比之下，中国网络上涉及经济的犯罪虽然不如西方国家那样频繁猖獗，却也是日渐嚣张。早在1999年，郝景龙、郝景文兄弟利用计算机进行网上银行盗窃的案件就已经引起举国震惊。

郝景龙身为中国工商银行江苏镇江分行花山湾分理处的职员，其工作职责便是维护银行的存取款系统，保证系统正常稳定的运行。精通业务的郝景龙很快发现，如果有一段程序可以在银行的系统后台挂接，就可以绕过密码校验，直接进入到用户的存取系统。而作为软件维护人员的他，每天与银行系统的各个部门打交道，可以名正言顺地以工作需要为借口，随意挂接各种设备和调度程序代码。

精心策划之后，他与双胞胎兄弟郝景文密谋，先在工商银行下辖的储

蓄所以假名开设了16个银行账户，由郝景文出资购买了电脑并安装了电话和调制解调器。当年9月7日凌晨，郝景龙进入自己任职的银行，顺利地把自己早已编写好并调试成功的程序与银行的电脑系统对接，同时由郝景文在自家的电脑上操作软件远程进入工商银行中心管理系统，分别向那16个银行账户打款共计300余万元，随后二人分别在扬州等地的工商银行储蓄所分期分批提取现金160余万元，后在某处储蓄所提款时被工作人员要求出示有效证件，二人担心事情败露，遂潜回镇江。

1998年12月，二人罪行败露，被判处死刑及无期徒刑。这也是中国有史以来第一次以电脑网络犯罪处以极刑的案例。

⑥ 莫让浮云遮望眼

证券业进入寻常百姓家时，股票早已由最早的传统交易方式转变为电子商务，纸质股票退出了历史舞台。中国自股票市场开通之后，黑客事件便层出不穷。

2007年夏季的一天，浙江金华的股民张某到公安局报案称自己投资3000万元购买的股票被莫名其妙地抛售一空，仅余940多万元在账上。张某声称自己炒股所用的银行卡一直随身携带，密码也从未透露给任何人，自己在这些股票被卖出时一直出差在外地，根本没有进行任何交易。经证券交易所查证，就在半个月前，有人用交易卡委托的方式在峰值处买入1900余万元的股票，随着股市下挫和不断地买进卖出，张某的2000余万元人间蒸发。后经证券交易所与公安部门查实，证券交易所没有任何违规现象存在，一定是某个熟知张某股票信息内情的人在暗中搞鬼，而张某身为某大型私企老板，平时得罪了不少商界人士，很可能就是这些商界对手窃取了张某的银行密码和股票信息，从而让张某的数千万元十几天里就在股市中化为泡影。

在随后的深入调查中，办案人员发现证券交易所的实习大学生耿某存在重大嫌疑，于是建议张某再投入资金以配合调查，并声称一旦张某的资金发生未知流动，将主动冻结，以保证张某不受损失。就在张某继续投入了700万元之后，耿某在办案人员的精心布局之下终于落网，被捕时耿某在证券交易所使用的电脑就停留在受害人张某的登录页面上。

耿某本是个品学兼优的大学生，自幼家境贫寒，父母均有残疾，让儿子学有所成、出人头地是父母最大的心愿。父母经营着一个小小的超市，每天早起晚归挣钱供耿某读书，乖顺的耿某也不负所望，以优异的成绩毕业后又被保送攻读研究生，但急于挣钱回报父母的耿某放弃了继续深造的机会，转而进入这家证券交易所实习。

从未踏入股票大厅的耿某立即被这里的气氛吸引了。那些金链子比手指都粗的人们大呼小叫，每天从指缝间流出流入的钞票以千万计，对于一个初入社会的贫寒学生来说，这无疑是一种强烈的生存反差和精神刺激。

就在实习的第四天，他跟着师傅进入大户室维护系统时偶然发现，这些财大气粗的股民们大多都是电脑盲，有些随手投入上亿资金的用户，居然连回车键在哪里都不知道。这让他灵光一闪，精于网络编程的他完全可以在用户无法察觉的前提下，安装一个小的密码探测软件，为自己开辟一个生财之道。

仅用了两天时间，耿某就编好了一个体积极小的密码探测器。这个探测器的工作原理是，当用户输入用户名和密码时，便把相应的按键次序记录到一个文本文件里，然后上传到耿某自己建立的网络空间里随时供其取用。

耿某最初的想法是直接套取用户的现金，但似乎这样做的风险太大，于是他转而想到利用这些用户的巨额资金，或高价买进，或低价卖出，从而拉动某只股票涨落，自己就可以从中渔利。

他东拼西凑了6万元钱为自己开设了股票账户，并以极低的价格买入若干股冷门股票，然后借助盗得的用户密码，以交易卡委托的形式大幅买

卖这只股票，让这只股票在极短的时间内把股价拉升到一定的高度，然后自己在高点卖出，再回过头来重新拉动另一只股票。如此往复，在短短的数月之内，耿某的6万元资金已积累到24万余元。

耿某最终为他的行为付出了有期徒刑7年的代价。一个前途无量的大学生，就这样一头栽入深渊，成为股市浮云的牺牲品。

【黑客知识】

霍克的“四舍五入”案：霍克名气不大，也算不得纯正的黑客，但其头脑灵活，手法可以算得上是高超巧妙，其“四舍五入”案曾经红极一时，成为黑客界经久不衰的经典案例。

1987年，霍克大学毕业，顺利进入加拿大一家银行做软件工程师，负责银行系统软件的维护和开发工作。在这期间霍克发现银行的财务系统中有一个很有趣的现象：在计算“我欠别人”时，只舍不入，而在计算“别人欠我”时则四舍五入。这样同一笔账目在“我欠”还是“别人欠”的计算中，总会有些小差别存在，而这些小差别虽然每笔数额仅几毛钱，但银行每天庞大的交易量，积少成多，这仍是笔可观的款项，天性聪明却又胆小怕事的霍克于是动起了脑筋，他利用职务之便，把这个银行界沿袭已久的计算公式顺理成章地加入到银行的利息计算程序中，同时在程序代码的最后，他有意加入了一小段指令，这段指令的作用就是把银行每一笔“我欠”还是“别人欠”的差额都转存到自己的银行户头上，这样每个月霍克的银行卡上都会多出几千美元，而霍克本人也心安理得地享受着这笔小小的入账自得其乐。

直到三年之后，银行因为扩大业务，又招募了另一个小伙子和霍克一起负责银行系统软件的维护工作，这个小伙子才无意中发现了霍克的这个小把戏。

打“时间差”的康尼：每个网络金融犯罪者，几乎都有着令人意想不到的犯罪手法，其中很多人更是利用了人们“计算机总不会犯错”这种习惯性的思维方

式，从而谋取大量不义之财。而在这些形形色色的网络经济犯罪方式中，康尼的手法无疑是独一无二的。

大学毕业后的康尼一直在一家规模不大的磁条加密厂做工人，虽然他不是计算机专业出身，但因工作需要，他透彻地了解生活中非常常见的磁条加密制作过程，这些磁条被广泛地应用于银行卡、考勤卡甚至餐厅的饭卡上。做了一年之后，康尼对自己的生活开始变得极其不满意，于是脑袋灵光的康尼在经过一番苦思冥想之后，想出了一个绝妙的方法。

康尼先在纽约的一家银行办理了一个私人账户，然后存入了数百美元，并要求银行开具了他的私人支票，利用这些支票和他在磁加密工厂的工作经验，他把其中十余张支票的磁条更改为自己刷制的磁条，那些经过更改的磁条上的银行特征码被刷成了旧金山的银行。康尼先用这些更改之后的支票到康涅狄格的银行兑换了一百美元，但康涅狄格银行的计算机识别系统验明这些支票属于纽约的银行，于是将其自动转到了可以通况纽约银行支票的别家银行，别家银行的计算机系统又识别这些支票应该来源于旧金山，于是自作主张地将其打回到旧金山，而旧金山的银行因为康尼的磁条信息虽然属于本地，但在本地的银行信息库中找不到对应的存款信息，于是自动将其删除，美国银行的惯例是被系统删除的银行支票为了防止误删会转为人工识别，负责识别这张支票的职员则通过支票上的银行地址认定这张支票来自纽约，于是人工将其拨回到纽约，随后纽约的银行则又重新开始了一次新的循环，而康涅狄格的银行则又不断地接到康尼的支票，并不断地为其付款，直到后来康尼被捕时，这张支票还在不断地被循环确认之中，而康尼就在这些支票不断地被反复确认过程中（系统并没有报告支票是伪造的，因为系统还在不断的确认之中）早已利用其他的支票透支了多达20万美元。

——第十章——
因为我们的存在世界才有进步

最让我们束手无策的也许就是那些躲藏在网络背后的无处不在无孔不入的电脑黑客，即使是最优秀的程序员也不敢说自己的程序没有可供黑客利用之处。若单纯以计算机技术水平来说，只有黑客，才是这方面最优秀的，因为我们在补漏洞，他们在发现漏洞，而且他们永远比我们快一步。

——比尔·盖茨

1990年的夏天似乎较前几年要热得更多，过低的气压把人的胸口压得透不过气来，每个人都昏昏沉沉提不起精神。

不过有件事却勉强算作调剂，KIIS调频广播正在如火如荼地进行一场收听率极高的广播。

主持人声嘶力竭，每个听众都明显地感觉到他的沙哑，但人们似乎并不太关心他的噪音是否美妙，人们更关心谁是第102个打进电话的幸运听众。

“看啊看啊，我们的电话声此起彼伏，听众们的热情就像这盛夏夜的灯光，它持久地闪亮，那些灯光装饰了我们的城市，而您的电话，却装饰着无数人的梦。现在，哦！让我数数看，是89，这是第89位听众，请问您

今天晚上的心情怎么样？”

没有人太在意这位听众今晚的心情，每个人都紧握着听筒，不断地拨打那部热线电话，不过似乎很难，那电话总是占线。

在离电台不远的一辆敞篷货车里，一个穿着随意的年轻人戴着耳机，旁边的收音机里，主持人还在不断地数着打进来的电话，并不断的询问每个人的心情，现场似乎有些火爆过头，嘈杂的声音与纷乱的心情几乎可以称得上是残忍地交织着，搅得人心浮气躁。这个年轻人手舞足蹈，嘴里低低地念叨着什么，把副驾驶位置的一台连接着很多电线的铁盒子上的闸刀开关不断地打开合上，又不时地在连接这个外形怪异的铁盒子的一部电话上按下那部热线的号码，兴奋地擦着脸上的汗。

“99，100……接下来，然后……”他瞪大了眼，深深地吸了口气，然后猛然把手中的闸刀开关压下去。坐下来，细细地倾听着耳机中的广播，似乎忘记了呼吸。

主持人的声音显然越来越激动。“我们已经……哦，让我确认一下，果然，这是第102个电话，我们期待已久的那个幸运儿会是谁呢？让我来报出他电话号码的后四位。他就是……”主持人故作神秘地拉长了声音，“他就是，4439的朋友，还记得我们的大奖吗？那辆红色的法拉利就在电台门前的停车场上，导播告诉我，这个幸运者10分钟之内就会赶到电台，我们一起期待他的出现吧。”

货车里的年轻人双臂上扬，做了个兴奋已极的欢呼动作，他摘下耳机，把电话听筒压在耳朵上，声音里压抑不住的颤抖。“是我吧？是我吧？那台法拉利跑车，我梦寐以求的座驾。哈，我要死了，等我找找身边是不是准备了氧气。”年轻人打开那个铁盒子，从中取出一块焊接着若干电子元件的集成电路板，放在嘴边亲吻着。

“宝贝，知道吗？你值一辆法拉利，你今晚的表现，真的太棒了。”

1 幸运听众

监听并控制电信局的电话，对于这位幸运听众卡文·柏森来说简直太不值一提了，通过监听并随时切断和接入某个电话系统，在那个晚上凭借他堪称卓越的黑客技术为自己赢得了那辆法拉利跑车，却着实让这个号称“幽灵”的顶级黑客兴奋了很久。

1982年，柏森的课余时间在一家规模不大的计算机公司做兼职操作员，由于其超凡的计算机知识，3个月之后就得到了升职，他的老板约见了他。在谈话中，他们对电话系统的热衷使得二人成为莫逆之交，并“合伙进行了一些有如战争般精彩的黑客活动，他给我买来一大堆技术手册，我对于黑客的兴趣由此达到了顶峰，技术水平也达到了一个新的高度”。

1983年，17岁的柏森第一次为自己的黑客行为付出代价，他被指控在之前的半年时间里，非法入侵五角大楼的计算机系统以及不少于16个军工项目组并试图窃取其中的相关军事机密。因为柏森尚不够服刑年龄，当局仅仅是没收了他的计算机，并让他的父母签订了一张保证书，以监护人的身份保证这个一旦拥有键盘就谁也无法控制的孩子不要做出什么出格的事来。然而对于一个“生下来就注定会成为天下第一黑客”的计算机天才而言，没有电脑的日子，根本是无法想象的。

这种事情在当时来讲简直是太不可思议了。人们在对他的电脑技术大加赞叹的同时都对他敬而远之，甚至在超市的收银台前，那些售货员甚至要求他与收银机保持1米的距离以防止他捣鬼；他所在的学校也毫不客气地将其劝退，但这并不妨碍柏森继续向最优秀的黑客看齐。“他们试图把我变成一个游离于社会之外的人，任何事都要拒绝我，于是我只有采取我自己可以的方式让天平向我倾斜。我有自己的利剑，它可以裁决一切。”

1985年，柏森伙同阿尔法·吉尔诺挂接了位于新泽西州的一家国际商业联盟的电话系统，并将其中包含重大商业机密的电话录音出售给巴西的

一家公司，从中获利43万美元。同时，柏森利用他对电脑的透彻理解，编写了至少16套电话窃听和搭接软件并在网上兜售，使得至少6000分钟的国际长途电话被认为是免费的内部电话而分文未取，泄漏的商业机密则无法具体测算损失。那些软件上，柏森骄傲地署上自己的大名，它们体积小巧，运行稳定，成为后来几十年里几乎所有电话黑客都人手一份的重量级武器，由此，柏森的名字如日中天，被遍布全球的数10万电话黑客顶礼膜拜。

1987年9月，柏森与吉尔诺酒后戏言声称要在一个月的时间里拿到贝尔安全设备公司的语音加密系统的核心技术，并邀请黑客圈子中的数位德高望重的前辈做裁判。在随后半个多月的时间里，二人先是编写了一套专门针对贝尔公司的电话语音解密软件，并成功地植入贝尔公司的中央计算机。贝尔公司开发了世界上最严密的语音加密系统，这套系统可以在特定对象的电话通信期间进行实时加密，也就是说，如果遭遇窃听者，若没有解密系统的工作，窃听者听到的只是些毫无意义的音节，根本无法知晓被窃听对象在谈什么。柏森的软件则巧妙地绕过了加密系统，以更高级别的优先运行权直接截获加密系统尚未进行加密时的声音信号并传送到柏森的耳机中，更巧妙的是，这个软件在运行之前会先判断此次通话是否为柏森已经挂接了收听设备的线路，如果柏森并未启动窃听录音装置，这套软件就会放过此次通话，只有柏森按下了录音按钮之后，软件才会启动，在加密系统之前拦截语音信号。

在不到一个月的时间里，柏森针对贝尔公司语音加密系统的主要负责人格林和比尔的通话录音长达400余分钟，这份录音资料里几乎包含了目前贝尔公司最新的语音加密系统的核心技术及弱点所在。格林和比尔显然在工作之余还在对自己负责的系统做最彻底的改进，并试图使其成为世界上最安全的语音加密系统。而柏森显然和这套所谓“绝无破解可能”的加密系统开了个天大的玩笑，柏森并没有费尽心神去解密这个系统，只不过在加密之前把最原始的声音信号抢先一步发送出来罢了。

幸好柏森只是出于玩乐，并没有把这份录音资料公之于众，但是在小范围的收听之后，那几位被任命为裁判的黑客前辈们郑重宣布，柏森和吉尔诺“干得真是太漂亮了，这是个堪称完美的动作，没有人会否认，这两个小伙子是世界上最懂得入侵技术的大师”。

❷ 窃听风云

随后的几年里，柏森不断地尝试新的电话窃听技术，并经常玩笑般把自己的电话听筒随意接到任意线路上，时而声称“太太，您订的蛋糕做好了，送货员将在10分钟之后按响您的门铃”。时而把一些通话加入到第三方通话当中，试想一对情意绵绵的恋人正在卿卿我我，电话里忽然传出一个苍老的声音，该是多么的搞笑和尴尬。在业余恶作剧的同时，柏森仍不遗余力地把耳机接入一些商业通话甚至是军事通话中，并从中获得“一些特殊人士会感兴趣”的信息以便从中谋利。更大的玩笑是柏森甚至把电话搭载到五角大楼的机密线路中，并在某一个清晨接入总统办公室，彬彬有礼地问候总统先生早安。

这个娄子显然捅大了，FBI开始把目光投到这个专门从事电话窃听和商业电话泄密的超级黑客身上，而这一切没有逃过柏森的窃听装置，他摇身一变，把握了十几年的电话听筒丢到一边，开始专业从事电子邮箱的破解。

侦听、破解、密码拆分这些事在柏森眼里似乎真的是毫无难度可言，只要柏森盯上了哪个领域，势必会引起一场不小的震荡。在柏森报复性地把FBI的往来电子邮件内容在网上公布开来之后，世界上没有哪一个使用电脑办公的人不知道FBI目前最主要的工作就是抓住一个身高六英尺三英寸的美国人，而柏森则由此真正名震天下，无人不知、无人不晓了。

只是知名度越高，FBI就越要除之而后快，毕竟面子上输不起。

柏森在破解了FBI的电子邮箱之后，转而进入了由军方管理的MasnNET计算机网络系统，并将其中一些敏感文件另存到一个至今无人发现的地方。在随后的疯狂入侵中，柏森挑衅般的针对FBI展开了刺探和破坏，他窃取了电信局分配给FBI的电话地址和分组号码段，并搭接电路进入了国家安全局的保密电话系统探听对他本人的案情进展情况。与此同时，他不但截获电子邮件，还中止了美国空军司令部对FBI及其他部门的绝密级往来电子信件40余封，“严重地威胁了国家安全，践踏国家法律，把商业秘密和军事、警备机密作为商品进行非法销售并从中获利”。为此，柏森在一家电信局的营业厅动用无线电干扰器进行非法挂接时被捕，法律给了他一个公正的裁决：五年监禁，并判处八年内不许碰触电脑、电话及无线电设备中的任何一件产品。

出狱之后的柏森与他的父母住在一起，家里的电话被拆除，电脑被当局没收，甚至带电子控温功能的热水器也被强行改为一台靠电热丝来加热的、经常让电闸罢工的蹩脚玩意儿。没有哪一家公司敢聘用他，因为世界已发展到计算机时代，几乎所有的事情都要依靠计算机来完成，而一旦天才的柏森接触到计算机，没有人会知道他会闯下多大的乱子。无所事事的柏森不得不每天把自己关在家里，甚至当他不得不去图书馆借几本书来打发时间的时候，也只能请图书管理员把计算机索引中的文件名称调出来供他筛选，而事实上，他的计算机技术可能比这位图书管理员强上一万倍。

20世纪八九十年代，电脑黑客界一提起柏森这两个字没有人不肃然起敬。在柏森时代，任何与电话、通信有关的行业都草木皆兵，甚至有专家级的人物声称，有柏森这样的电话黑客存在，势必会让传统的有线通信业在极短的时间内消失，从而更大限度地促进互联网通信的发展。

而柏森则说，“正因为我、我们的存在，世界才在前进。”也许全世界也只有柏森一个人敢说这样的话，有资格说这样的话。

这话多少有些大言不惭，但却又不无道理。

❸ “战神潘戈”

与卡文·柏森齐名的电脑黑客除了前文提到过的米特尼克之外，似乎只有潘戈能与之并肩。

潘戈不像柏森那样热衷于电话系统的入侵，也不像米特尼克只知道与警察捉迷藏，他要干的是些惊天动地的大事。如同所有认为仅凭一己之力就可以拯救世界的人一样，潘戈的事业很伟大，他经营着一项平衡世界的计划。

潘戈原名汉斯·亨里克·胡伯纳，1968年出生于西柏林。正处在战后重建的德国到处瓦砾遍地，社会经济尚处在恢复的过程之中，幸好汉斯的父母经营着一所不算大的农场，至少可以让他吃饱肚子，但祖国分裂、民不聊生的现状还是让小小的汉斯有无法释怀的郁闷压抑在内心。

20世纪80年代，英国率先在西柏林开设了电脑公司，并大量引进计算机，把计算机作为办公设备的一部分将西柏林带入现代化的办公环境中。在那个时代，计算机这个新生事物价格昂贵，除了一些实力雄厚的大公司外，家用计算机是让人望而生畏的奢侈品。汉斯第一次看到计算机是一个来父亲农场做推销的电脑公司业务员，他随身带有一台便携式笔记本电脑和几本操作手册，然后在父亲的办公室里夸夸其谈计算机的种种神奇，父亲显然对这东西并不感兴趣，倒是一旁的汉斯，目不转睛地仔细聆听了推销员的讲解和演示，然后在推销员的许可下第一次上机操作，之后就不可救药地爱上了这冰冷的东西。

在自己的一再要求下，父亲最终给他买了一台电脑，随后汉斯就一头扎到各种计算机书籍中，不分昼夜地敲击着键盘，以至于三个月后父亲不得不给他重新更换了键盘。在翻烂了那几本薄薄的电脑手册之后，汉斯开始尝试着自己编写程序，在他的努力下，父亲平日要三五天才能完成的农场工人的工资核算，他只用了半小时就整理完毕。这让父亲感到很惊喜，

从此小汉斯在电脑上的任何要求，父亲都无条件满足，这让小汉斯在短短的时间内就成为远近闻名的电脑高手，甚至不少大公司也时常找他来调试程序、修理故障，而农场工人的孩子们也众星捧月一般围在他身边，向他请教计算机知识，后来汉斯索性在自己的卧室里开办了一个小型的电脑培训班，每周教授两个下午的计算机课程。

那一年，汉斯只有14岁。

除了钻研计算机技术之外，汉斯平时最喜欢玩一种叫“潘戈大战斯诺比”的游戏，学校里能和他在这个游戏上一较长短的只有一个叫尼莫的男孩子。尼莫知道汉斯电脑水平高超，也有意结交，在尼莫的生日那天，汉斯接到了尼莫的邀请，并在尼莫家里第一次知道了“调制解调器”这个名词。

那是一种方盒子，上面连接着电线，并有一个接口与电脑相连，当时调制解调器的传输速率只有几K，但这却是当时唯一一种可以连入互联网的设备。当尼莫打开开关，用这个闪着提示灯，不时发出几声怪啸的东西链接到西柏林的电子公告板，并在上面即时与在线者交换对时政的看法时，汉斯张大了嘴，他隐隐感觉到另一个隐藏在电脑背后的更加神秘和充满诱惑的世界已为自己敞开了大门。在尼莫的指点下，汉斯第一次在网络上留言，而当尼莫告诉他可以给自己取一个网名的时候，汉斯毫不犹豫地把自己称作“潘戈”。

似乎所有最初接触电子公告板的人，都有意无意中被指引着入侵某个系统，潘戈也不例外，事实上最早的电子公告板，本身就是一个黑客经常出没的竞技场和黑客技术的交流园地。一周之后，对计算机有着天然敏锐直觉的潘戈就独自完成了第一次成功的黑客试验，他的牺牲品是麦道公司设在美国西海岸的迪姆网，潘戈在修改了网站的首页之后，“战神潘戈”从此开始了独步天下，傲视群伦的黑客生涯。

1985年2月，长久以来一直牢牢控制着迪姆网的潘戈，通过“友情链接”点击了美国斯坦福大学的高能物理科研中心网页，并立即发现了这个科研中心系统中直线加速器系统页面里，存在着一个溢出型漏洞。当潘戈

在留言板上善意地提醒网站存在的危险之后，让他意外的是，网站的管理员立即做出了反应，并与他在留言板上亲切友好地交流起来，管理员抱怨说工资实在低得可怜，而潘戈则对自己的黑客故事津津乐道。若不是另一个脾气暴躁的管理员毫不客气地让潘戈“立即滚蛋，在直线加速器主页面消失”的话，潘戈对这个夜晚还是相当满意的。

从小到大，仅在计算机技术上没有人敢如此嚣张地对潘戈出言不逊，相反，潘戈早已习惯于被人崇拜和尊敬。第二天一整天，潘戈闷闷不乐，埋头于电脑前用不到三百行的代码编写了一个冗余循环程序，并借助昨晚发现的那个溢出漏洞将其植入直线加速器系统页面。这个程序在向系统后台发出一个请求接入的信号之后，就立即把自身分裂复制一份，然后这两个程序一同向系统后台继续发出一次请求接入的信号，再分别复制一份，再重新进行接入请求。几何级的分裂和递增的接入请求，在极短的时间内就会使系统的资源耗尽，进而崩溃。随后，他修改了系统主页面，并依照惯例留下了自己的大名，“如同与上帝吵架一样，在电脑前，在潘戈的身边，你最好沉默，否则潘戈将如附骨之蛆般如影随形。”

这份警告唯一真实之处就在于，真的如他所说，在电脑前谁惹恼了潘戈就会有无尽的苦难不请自来。

4 平衡世界的计划

19岁那一年，潘戈显然感觉到缺乏挑战的刺激以及赢得胜利的快感，有一段时间他甚至心灰意冷到连电脑都不想碰的地步。“网络不过如此，再没什么值得我留心的了，没有什么可以在面前阻挡我。我似乎缺少一个目标，缺少一个值得我注意的对象。”

整个夏天，潘戈游荡在西柏林的大街小巷，每天和挑夫、花匠混在一起讨论防晒的秘方和花土的养分与施肥量多少的关系，每晚把自己弄个大

醉。他没有考大学，所有的学业在他眼里都止于电脑，除此之外不会再对其他什么感兴趣。在浪费了大半年的时间后，一个偶然的机会，尼莫给他介绍了一个经常在汉诺威集会的黑客组织“混沌俱乐部”。最初潘戈并不在意，在黑客这一行当里，更多的人热衷于骗钱和恶作剧，而这一切早已对潘戈没有了吸引力。当尼莫声称这个黑客组织的与众不同之处在于“和政治有些瓜葛”之后，潘戈为之一振。

柏林墙是政治斗争的产物，仅仅一墙之隔就是截然不同的社会制度。自小对于祖国分裂深感遗憾和无能为力的潘戈一向反感政治，但世界上的事情有时就是这样，当你反感政治的时候，一旦有机会你还是会热衷并参与政治，因为太久的失望之后，你会发现只有政治才是解决政治的最佳手段。

与混沌俱乐部的首脑海格巴德等人接触之后，潘戈的热情终于被调动了起来。海格巴德早有想法，准备与苏联人做些交易，他的想法是“我们有最敏锐的计算机刺探技术，而苏联也需要相关的机密技术资料以便在经济、军事上尽快赶超在某些方面比苏联更先进的西方国家。从美国的相关机构里通过黑客手段窃取情报出售给苏联，以使这两个超级大国在整个世界范围内继续保持均衡，实际上这是以黑客身份维持世界和平的一项伟大事业”。

潘戈与海格巴德将其命名为“平衡计划”。

1986年10月，海格巴德驱车前往东柏林的苏联驻德事务处理中心，并请求与主管人员面谈一项“商业计划”，随后一个自称谢尔盖的中年男人接待了他。在对方怀疑的目光注视下，海格巴德简单地做了自我介绍，强调自己是西德最大黑客组织的领导者，“我们可以搞到一些有趣的东西，比如入侵很多西方军事设施的计算机系统或是核能中心的网络等，并从中找到你们中意的东西。当然了，我们的报酬是按质论价的。”

谢尔盖显然被说服了，他先是回办公室打了大概20分钟电话，然后回来告诉海格巴德说，作为首次交易，要对他们的计算机能力做些考验，比如拿到美国阿斯顿·泰特公司为美国核能物理实验室编写的软件。

这确实有较高的难度，海格巴德召集了大约十名顶级黑客对泰特公司

的内部服务器进行了无数次的试探性入侵都无功而返，直到谢尔盖两周后致电要他“交出些成绩来让苏联人开开眼界”的时候，手中空空的海格巴德迫不得已决定带上潘戈，因为只有潘戈才会让他勉强有个交代：“看！虽然我们没能拿到泰特公司的软件，但我们有潘戈。看看吧，这家伙有多优秀！”

潘戈给谢尔盖带去了另一份见面礼：一个被业界称为“特权机器”的运行于VMS系统的程序。VMS系统一般应用于高机密的计算机系统，而这个程序正是运行在这个系统之上的，其功能在于一旦进入到某一管理环境之中并运行这个软件，就可以任意提升某一注册用户的权限，可以从最普通的一般用户提升为超级管理员，即只要有办法入侵某一VMS系统，便可以随意查看和增删系统文件，将受控计算机视为已有并尽取所需。

谢尔盖的脸上多少有些笑容了。虽然不能打满分，但混沌俱乐部的表现还是可圈可点的。

5 游走在克格勃与中情局之间

在接下来的两年多时间里，以潘戈为技术骨干的混沌俱乐部向谢尔盖及克格勃组织，移交了包括美军波尔克堡军事力量数据，及各大银行在美国的资金流通详细年报表等军事及商业情报达500多份。而潘戈平时很少与混沌组织的人接触，他深居简出，与最亲密的朋友和战友尼莫在西柏林经营着一家规模不大的软件公司，所出售的软件全部出自二人之手，每个软件的落款都有着二人名字的合拼字母“Panni”。每周六，潘戈会端上一杯加了冰的威士忌，登陆混沌俱乐部的电子公告板，给那些后辈小子们做一些最基本的黑客知识讲座，而尼莫则热衷于和那些黑客同行们做面对面的接触，他始终认为，以一个前辈的姿态出现在众人面前并找到众星捧月般拥戴的感觉，才是一个终极黑客的至高荣耀。

直到有一天，尼莫在办公室里接受了两个受当地警察保护的网络安全

专员的询问。询问直接从不久前尼莫入侵克利格斯的网络计算机终端一事开始，在历时一个小时之后才告结束，网络专员以法律的名义向尼莫下达了“禁止外出到西柏林以外的任何地方以便随时接受调查”的书面通知。尽管尼莫对答如流，在整个询问过程中表现得极为镇定，但他有理由相信当局有确凿的证据证明他犯有非法网络入侵罪和间谍罪。

这期间，潘戈就坐在一墙之隔的办公室里侧耳倾听着所有的一切。

在警察的严密保护下，两位大腹便便的网络安全专员礼貌地告辞离开。尼莫与潘戈一致认为尽早脱离混沌俱乐部以及断绝与谢尔盖的联系是当务之急。但当局显然是做了充足的准备，次日的德国《快捷》杂志就抢先报道了有关混沌主将尼莫涉嫌出卖国家机密、非法入侵商业及军事网站的消息，随后在西德发行的《纽约时报》也以连续报道的方式高度关注这一事件，甚至在其中一期中还刊登了一张尼莫在复印机前工作的照片，这显然是那些记者们通过窗口偷拍的。

潘戈开始坐立不安了，虽然当局现在仅仅是以尼莫为突破口打击了混沌俱乐部，但尼莫知道自己的一切秘密，只要尼莫稍稍放出口风，自己的罪就要比尼莫大得多，至少尼莫不会高尚到他一个人在牢里受苦而让潘戈在外面享福。

海格巴德解散了混沌俱乐部，在与潘戈简单接触了一下之后，随即消失了。

潘戈也从此销声匿迹，仿佛从来没有在这个世界上出现过一样。

❻ “我来过”

随着时间的推移，混沌俱乐部逐渐淡出了人们的视野，但那些署名“Panni”的软件还风行世界。不知所踪的海格巴德也似乎想在命终之前给这个世界留下一个“我来过”的印记，他出版了一本书，书名就叫《我

来过》，其中详细地描述了混沌俱乐部与谢尔盖为代表的克格勃组织进行种种交易的经过，书中多次提到这些交易中最主要的功臣——潘戈。

潘戈仍旧踪迹全无，人们只知道，他一定还活在世上，像他这样精明睿智的精英级人物，只要还没有被警察发现，就一定会很滋润地躲在某处风景宜人之地，一杯酒、一份报，开心自在地生活着。

作为黑客中最顶级的高手之一，消失的潘戈是最恰当也是最具传奇色彩的结局了。人们更喜欢这样一个结局，一个超级聪明的人，一个拥有超级本领的通天大盗，一个当局也对其无能为力的结局是最理想的结局。

而几乎所有的人都相信，每个从事计算机工作的人，每个试图学习黑客技术并热衷于黑客事件的人心中，都会给潘戈留下一个位置，一个非常靠前的位置，因为这个名字曾经在计算机世界光芒四射。

想诠释潘戈这个名字，可以复杂到写一本书，也可以仅仅用海格巴德的书名做最简单的概括：我来过。

【黑客知识】

溢出漏洞：电脑中的每个应用程序都是由程序员用编程语言编写的代码组成。在程序的编写过程中，由于程序员的人为错误，会使程序在被系统执行的过程中造成数据交换的错误，这些错误会导致系统运行的不稳定和程序的崩溃。比如一个密码输入对话框，程序员在编写程序的时候如果要求这个密码输入框内只接受6个字符的密码，而没有对不足6个或超过6个时编制相应的处理程序，那么这些超过的密码字符会覆盖掉随后输入的数据，这样系统就会发生错误，程序通常会被导入另外的模块执行。于是这种程序的错误就会造成所谓的系统漏洞，这种错误的发生在业界被称做数据溢出漏洞。黑客们会在所有的应用程序中寻找这种漏洞，在程序被溢出漏洞引向另外的模块运行之前，黑客操控这些程序的走向，并将其指向自己希望执行的模块或其他程序，以达到入侵的目的。

—— 第十一章 ——

一个传奇女子爱恨情仇的黑客生涯

永远不要忽视小人物，大人物一般有大胸怀，小人物没有，小人物通常会给你个大报复。

——苏珊

作为知名的黑客，苏珊在遇到罗斯科之前，还是一个电脑盲。

每晚7点，苏珊会准时出现在西雅图的红灯区，浓妆艳抹随时准备微笑。她是一个站街女。

苏珊算得上是个标准的美人胚子。一头金发和六英尺三英寸的身高足以让她吸引大量的目光。虽然每晚的生意好得不行，但她还是觉得手头拮据，原因在于她每月都要面对高额的电话账单。

她61岁的老母亲在伊利诺伊州的阿尔托那，每天早上会泡了牛奶一直坐在靠窗的位置上，直到等来女儿的电话。

苏珊的母亲是个盲人，在她8岁时，她那每天都要喝得酩酊大醉的父亲一记耳光让母亲的一只耳朵再也听不到声音了，于是苏珊每次打电话都不得不吵架一般扯着嗓门。

17岁，苏珊来到了西雅图，但是除了一副动人的脸蛋之外她再没什么资本了，甚至不能支付她在街边支起一个小吃摊的费用。她做过计费员，在小餐馆里每天想办法躲开食客们不怀好意的眼神、无端的谩骂和老板的

呵斥，直到有一天她把一整盘烤牛肉扣到一个大腹便便的秃顶“咸猪手”上之后，她终于有勇气站在街边冲每一个路过的男人招手了。她60岁的老娘在等着她挣钱吃饭。

对于苏珊而言只有两个愿望：一是挣到更多的钱；二是有免费电话供她使用。

1 因为爱情，走向深渊

20世纪80年代的美国，BBS已经遍地开花非常普及了。在BBS上，人们可以随意地结成社交团体，就某一话题畅所欲言。而这种可以穿越千里相聚一堂的方式立即受到强烈的追捧，很快一些黑客自觉地成立了相对固定的团体，在BBS上进行黑客技术交流。就当时而言，电话黑客方兴未艾，黑客们下大力气研究技术，只为了一个很现实的目的——免费电话。

苏珊也抱着同样的目的。她借了朋友的电脑，笨拙地在BBS上敲出一则交友信息：

“我是一个新加入的朋友，一个对电脑或是黑客一无所知的人，但我知道这里面有我需要的，于是我来了。很希望在这里认识一些对我们彼此都有帮助的朋友，随意打发那些无聊的周末，特别是能聊聊电脑技术。顺便说一句，我身高六英尺三英寸，金发，体重140磅，爱好到处走走，谁知道一些新鲜去处不妨告诉我，我是个很好的游伴和免费的导游。”

仅凭“六英尺三英寸”和“金发”这两个关键词就足够了。帖子发出去没几分钟，便有人跟帖自报家门，来者自称罗斯科，一个“擅长以技术切入电话系统，轻而易举便可以获得免费电话、免费机票，甚至免费早餐”的喋喋不休的年轻人。

罗斯科技术的确不一般，在整个西雅图地区的黑客圈里小有名气。在1980年的美国，真正可以不借助硬件而仅凭软件技术入侵就能得到利益的

黑客实属凤毛麟角，而罗斯科正是其中之一。在免费电话领域更多的人是借助于一种叫做“蓝精灵”的电子硬件设备接入电信局的操作线路实现免费通话的，他从来看不起这些只会使用工具而不会动脑筋的笨蛋，“蓝精灵”很容易被跟踪，而罗斯科眼中的真正高手应像魔术师一样凭空取物，而他本人正是这样的高手。

据说让他一夜成名的事件发生在大概半年前，他和朋友打赌，要让电话公司给他一笔数目不小的钱，结果他真的这样做了：罗斯科入侵了西雅图的电话系统，先在电子账单上修改了自己的通话记录，让系统误以为他本月共计使用了近500元的电话并付了相应的款项，然后他跑到银行打印出了纸质账单。第二天，他又进入系统将电子信息修改为很小的数值，然后拿着那张电话费单据找到了电信部门，一顿大吵之后，在经理不住的道歉声中趾高气扬地拿走了400美元。这件事不知被谁走漏了消息，当局很快锁定了罗斯科，而当时的法律还没有任何条文认为罗斯科触犯了刑律，罗斯科因此逃脱了惩罚，也因此成为名动一时的风云人物。之后不久，一位记者准备采访他，并通过一个黑客朋友向罗斯科转达了自己的意向。第二天，一个电话打到记者家中，来人滔滔不绝地把这位可怜记者的姓名、住址、银行卡信息和存款金额以及上中学时的成绩一一报出，最后得意地笑着自报家门：“我就是罗斯科。”

这样一个技术精湛，可以随意进出电话系统的黑客正是苏珊所需要的。没几天，她便和罗斯科打得火热，他给她打免费电话的技术指导，她则给他“六英尺三英寸的美丽和一头金发的刺激”。

各取所需永远是拥抱取暖的最恰当的借口和理由。接下来的日子里，苏珊晚上仍然是一脸妖艳地推门而去，深更半夜地返回来窝在罗斯科不足20平米的房间里通宵达旦地摆弄计算机。除了勾引男人上床之外，苏珊对如此“勾引”电话系统更是得心应手，很快苏珊就可以独立进入电信系统，随意地改变电话号码，把正在美国本土通话的某一方线路转接到连她本人都不知道的澳洲某个小山寨里去。或者，恶作剧般的让一些本来没有

安装电话的家庭莫名其妙地接到高额的话费清单，偶尔还会兴致所至打断别人的通话，插上一句“对不起，打扰一下！因线路改造的原因，您的电话号码已改为8-3-7-1/2，请问您会拨那个1/2吗？”然后哈哈大笑地跟罗斯科描述事主电话里张口结舌的样子。更主要的是，她可以随时跟母亲聊上一个上午而不用总是盯着墙上的时钟计算时间和话费了。

这时的罗斯科已经不仅仅只对免费电话感兴趣了，小小的电话系统在他眼里不过是小儿科，丝毫提不起他挑战的欲望和胜利感。顶级的黑客总是惺惺相惜的，于是毫不奇怪，罗斯科和大名鼎鼎的世界第一黑客凯文·米特尼克结识了，两个同样对黑客入侵有着深入研究的人决定强强联手，把触角伸到了中央情报局、美国航空航天局等敏感性、机密性、技术性更强的系统上去。而苏珊也结束了每夜都出去站街的皮肉生意，在一家不算大的电信公司做接线员，偶尔去罗斯科的小屋坐上一坐，并自然而然地开始了她的第一段爱情，令她倾心的自然就是长得高大帅气的、在黑客圈子里堪称宗师的罗斯科。

每个女孩子都把自己的初恋看得重于泰山，也都全身心地投入和付出；但事实上她错了，似乎这世界上每一个初恋故事都是一个美丽的让人心碎的错误。

这时的苏珊已经不太看中金钱了，做接线员虽然辛苦但还算稳定，收入也还令她满意，毕竟和母亲的免费电话让她少去了一大块经济负担，她甚至想等和罗斯科结婚后把孤苦的母亲接到西雅图来过几年滋润的日子。每获闲暇时，她会扯上罗斯科去街上的咖啡屋坐上几个小时，听听音乐或是就那么挽着手走走、看看夕阳，但这时的罗斯科除了神游物外、口中念念有词地叨咕那些黑客专用名词外，就是计算某个密码的破解次序，实在大煞风景，时不时还会扯上腰围比裤子还要长的凯文。苏珊兴趣正浓的时候，两个人却蹲在一边饶有兴致地给他们遇到的各大网站的入侵难度打起分来。

渐渐地，罗斯科不再每天出现了，理由是大学即将毕业，他要忙他的

毕业论文。罗斯科常是三更半夜回来，一身酒气，甚至领口上还会沾上口红。

“我就是这样兴致勃勃死心塌地地要嫁给一个拈花惹草的酒鬼吗？”苏珊的质问经常只换回来一声嗤笑。

隐隐地，苏珊感觉到一股末日来临般的恐惧，在罗斯科布满红丝的眼睛里，她感觉到了自己视为纯真的、至高无上的爱情，即将枯萎。

❷ 最不可笑的玩笑

常混迹于黑客圈子里，苏珊也结识了很多黑客朋友。在那个小雪不止的傍晚，当她接到了一个名叫罗兹的黑客朋友的电话后，她知道自己的预感已经成为现实，罗斯科真的不再迷恋于“六英尺三英寸”和“金发”这两个名词了。

罗兹无意中监听到一个电话，是一个女人打给罗斯科的。电话里罗斯科向那个女人求婚，并要求这个女人把他弄到她父亲做总裁的公司里去。显然那个女人并没有反对，甚至反问：“那么，你的花呢？我是说，我早就向你说过的，如果求婚，我要镶嵌着绿萝草的红玫瑰。”

这是个富家女，并且出身很好，有着优秀的贵族血统和良好的教育，她可以给罗斯科一个步入上流社会的最好契机，而苏珊除了“六英尺三英寸”外一无所有。

“你们根本不在一个重量级上，苏珊，我的好姑娘，我看你还是趁早放手。要知道，青春我们浪费不起，你偷得到任何东西，但青春，不仅不免费，你还偷不到。”罗兹虽然20岁不到，但说这话的时候忧心忡忡，担心的神色浓得化不开。

“没有良好的教育，没有高贵的出身，但这不是我的错，相反我积极向上，我乐观坚强，我有一个好母亲和一个曾经很爱很爱我的电脑技术

一流的男朋友。但是我现在必须要失去其中之一了，就像长途的马不堪重负，必须要舍弃行李中的一部分，而这些要舍弃的东西，却不是由我来选择，这是第一个玩笑，也是最不可笑的玩笑。”

苏珊整个人都暗淡下去，每天百无聊赖地敲着键盘，在BBS上看那些熟悉的朋友们嘻嘻哈哈地谈笑风生，偶尔罗兹会悄悄发过来几句问候和关心，“我最不喜欢看到一朵花的凋谢，但是春天过了。”

“嗯，春天过了，我的季节没有夏天；冬天来了，我也许即将死去。”苏珊回答。

偶尔苏珊会跑到街上去，等在罗斯科每天必经的路旁。西雅图的冬天很冷，大雪有时令人感到恐怖。

罗斯科经过的时候，两个人会默默地对视很久，谁也不开口，直到雪开始在脸上融化。

“我们结婚吧。”有几次，苏珊平静如水，似乎很随意地试探，但罗斯科闪烁其词，顾左右而言他，被问烦了就会抽身走开。再后来罗斯科干脆再不露面。

如果天真的苏珊懂得放手，事情便不具备任何传奇色彩了，但是苏珊太看重这份感情了，毕竟，初恋对于一个女孩子来说，足以感动终生。苏珊在罗斯科的电子信箱里留下了一封措辞严厉的邮件，声称如果他再不出现，她就把他入侵政府系统的事捅到FBI那里去。

对此罗斯科嗤之以鼻，这个来无影去无踪的黑客领袖，一向以神龙见首不见尾自我标榜，FBI又能耐我何？

罗斯科的回信只有一句话：“你尽可以做你想做的。”

❸ 跟凯文·米特尼克叫板

1980年的圣诞节，人们都在忙于采购圣诞礼物的时候，西雅图最大的

零售公司CES公司的销售系统却莫名其妙地发生了一些小故障。一盒牙膏居然卖到20美元，而一台日本原装的彩电，经系统扫描，只需要付15美元就可以拿走。系统管理员立即向销售系统软件经销商汇报了情况，技术人员声称整个西雅图的CES公司销售软件都出现了故障，需要使用者提供系统的登录名和密码以便维修。管理员毫不犹豫地照做了，过去也经常这样和他们合作的。这些小子的技术还真过得去，通常第二天系统就会恢复正常。

第二天早上，情况更糟了。连接电脑的打印机显然是工作了一整夜，店里满地的打印纸，上面密密麻麻写满了诸如“我是你驱之不散的幽灵，你们的系统号称无懈可击，但在我眼里小菜一碟”之类的话，下面赫然留着罗斯科和米特尼克的大名。

“这下，给你干了个漂亮的。”

面对苏珊的这封简短的电子邮件，罗斯科不以为然。“尽管放马过来吧，罗斯科就在你的指掌之外，能奈我何？”

接下来苏珊与罗斯科的争斗便转入白热化。一个绝望女人的报复，通常是最彻底的。

在连续破坏了数家连锁超市的销售系统之后，苏珊转而施展她从罗期科那里学到的电话入侵手段，模拟罗斯科的手法不断地把电信局的接线员搞得焦头烂额。

而这个时候，正是米特尼克在下村勉的追击下节节败退之际，米特尼克特别想扭转不利局势，因此他频频与罗斯科取得联系，倚仗着罗斯科高超的电话入侵技术试图截获下村勉的电话记录，以求得到他下一步的攻击方位，罗斯科也想在这场势均力敌的斗争中一举取得胜利来奠定自己的黑客霸主地位。他每天蹲在椅子上，头戴耳机、手握键盘，认真得像一个被罚抄作业的小学生，根本没有心情理会苏珊的捣乱，这让苏珊很是得意。虽然苏珊找不出罗斯科的具体位置，但她至少可以趁火打劫一下，她要的不仅仅是罗斯科付出爱情的代价，更要在黑客圈里，把罗斯科搞臭搞垮。

苏珊不断地把她的电话线路接通到罗斯科的专用线路上，然后把录音内容逐一分析后发到位于佛罗里达州的一个黑客BBS上，在那里罗斯科与米特尼克的每一次网上联系都被公之于众，而发布这些消息的注册人名为“克迪玛”，正是那个与罗斯科打得火热的富家女的名字。

再后来，苏珊截获并公之于众的罗斯科与米特尼克的对话记录里，经常会出现二人对骂的情节，米特尼克骂罗斯科是头蠢猪，害得他总是被下村勉追得团团转，而气急败坏的罗斯科在痛打了克迪玛一顿之后，发现这个只会发嗲的富家女对黑客行径根本就是一无所知，而米特尼克那边却还以为罗斯科自己在用女友的名字给自己打广告、做宣传。

罗斯科与米特尼克交涉几次之后，早成了惊弓之鸟的米特尼克俨然失去了耐心和兴趣，他不再相信罗斯科，并在BBS上公开声明自己与罗斯科的决裂，然后不辞而别，丢开了罗斯科这个对于电话入侵堪称祖师的大师级人物而一个人隐身于网络之中，在与下村勉的对决中，主动把自己降到了弱者的位置上。

一直严密监视罗斯科的苏珊见状大喜，她知道自己已经成功了第一步，接下来她要亲手毁掉罗斯科那前程似锦的爱情。

4 被低估的姑娘

罗斯科终于可以穿上名牌西装、每天夹着公文包、油头粉面地进入摩天大楼成为白领一族了。克迪玛的父亲把这个帅哥安排在自己的公司做行政副手，掌管公司中层人事分配。这职位看似并不重要，但却让很多人眼红，因为但凡中层人事变动，都要经过这名天才黑客的首肯。

每个傍晚，苏珊都会躲在公司对面的咖啡屋里，握着一杯凉透了的咖啡，目不转睛地盯着罗斯科把公文包丢进那辆深灰色的雪佛兰汽车里，然后发动车子，掉头回到公司门前，克迪玛自然会适时地出现在门口，先是

亲热地搂着罗斯科热吻一下，再钻进车子……夕阳的光芒从远处的山上斜射过来，万道金光之中，那辆雪弗兰会像鱼一样游进车流转瞬即逝，不远处的屋角上，一只猫正盯着街上的行人发呆。

苏珊也在发呆，那个拥吻罗斯科的人应该是我才对。

那些甜得像蜜、浓得化不开的温情日子，那些在电脑屏幕前的一个个惊心动魄的夜晚和随之而来的无尽缠绵，回忆之门在苏珊眼前轰然开启，而恰恰是这些看似美妙的回忆，蚕食着她饱经风霜的心。

依靠着从罗斯科那里学来的电话入侵技术和自己一头金发覆盖着的满脑子智慧，苏珊几经尝试，终于把自己的电话终端接上了罗斯科的办公室。除了用罗斯科的办公电话随意拨打长途外，苏珊还把罗斯科的电话做了录音，他的每一笔业务、每一个人事任免，苏珊都做了详细记录，然后她开始设法接近那些相对比较重要的中层领导，暗中把这些消息透露给当事人。当然，作为一个资深的站街女，仅凭苏珊的身高和秀发，在某个酒吧或类似的场合里与一些中层领导制造一场“巧遇”并熟识显然并非难事，她希望这些人能在自己的能力范围之内并在他们离职之前，替她做些什么。

那些一直认为自己正在被公司重用的中层领导起初对苏珊的消息不置可否、半信半疑，但渐渐地总会感觉到事情正如苏珊所说的一样，公司比较重要的会议再也不让自己参加，一些重大决策自己甚至毫不知情，过不了几天就会被罗斯科单独叫到办公室里谈话，再后来这个人就会悄然消失。

几次三番之后，与苏珊结识的中层领导们都对苏珊的预言深信不疑，甚至经常约苏珊出来打探消息，而苏珊总不让他们失望。久而久之，这些心中七上八下的男人们便众星捧月一般把苏珊奉为神女顶礼膜拜，只有罗斯科还蒙在鼓里。只是这些男人从来没注意过一个细节：这个预言精准的神秘女人，从来不用电话。

苏珊知道，作为电话黑客的鼻祖级人物，只要自己一接触到电话，罗

斯科准会知道自己的行踪。就像几个月前，罗斯科和米特尼克把一个无线电发射器挂接到苏珊的电话上，在一番无耻的窃听和录音之后，把音频资料上传到了BBS上供那些黑客们取笑，罗斯科甚至嘲笑苏珊是个不要脸的妓女。“她廉价到1个小时只需要花费你20美元，而她的服务绝对是第一流的，作为她的第一任男友，我想你们会相信罗斯科，这个大名鼎鼎的黑客的话。”

而他当初得知自己做妓女完全是为了妈妈的生活时，甚至还怜爱地揉着她的头，夸赞她是个乖孩子。每每想到这些，苏珊就气得浑身发抖。

她所能做的就是，同样在BBS上公开宣称罗斯科其实是当局的密探，其存在于黑客圈里的意义就在于，随时掌握黑客的最新动向等相关信息并随时报告给他的上级，包括他貌似热情地帮助米特尼克躲避下村勉的追击，而“实际上每天给下村勉先生报出米特尼克所住旅馆的门牌号，这也是他们两个人从好到不能再好的朋友变成现在恨不得杀了彼此的原因”。

罗斯科对现代化公司的管理还算有一套。长期混迹于无论在思想，还是社会敏感度都比较前卫的黑客圈子，罗斯科对于社会发展及公司运营的前瞻性把握得恰到好处。像擅长发现电话系统的漏洞一样，他对于公司人事的敏感同样是超一流的，他会在极短的时间内正确判断一个中层员工是否适合本公司的经营模式以及是否忠心，然后果断地做出任免决定。在罗斯科上任半年之后，他已经把公司的中层领导几乎换了个遍，提拔了一大批年轻有为的人，为此公司中层硕果仅存的几位元老如坐针毡，谁也说不准哪天就会自身难保。

苏珊于是在她接触的中层领导中，故意提到波兰一家跨国公司对某某产品极有兴趣，而这个产品正是罗斯科公司的主打产品，其生产技术和配方是严格保密的。这个消息对于这几位深感不安的公司中层领导自然极具吸引力，这几个愚蠢的家伙不仅对苏珊的预言深信不疑，得知她的这个消息后也自然表示愿意与波兰方面接触，而这一切都交给苏珊代劳。

在苏珊暗示这几个中层领导的末日就快来临的时候，这几个人也终于

费尽力气把配方搞到了手，并由苏珊卖给了波兰方面，当然他们每个人都得到了一笔数额不小的酬劳，在拿到了这笔足够养老的钞票之后，几个中层领导抢先一步很体面地集体辞职了。

❺ 胜利的代价是悄然退场

在一个午后，苏珊故技重演，侵入了克迪玛的办公室。当克迪玛吩咐秘书把自己的泳装准备好时，苏珊抢先来到了公司门前，现在她特意换上了一套快递公司的工作服。

门卫自然禁止苏珊进入公司，而苏珊则施展美人计，在几分钟之内与门卫打得火热。当克迪玛的高跟鞋一声声清脆地敲击大理石地面的声音逐渐变得清晰起来时，苏珊立即冲门卫甜甜地微笑着向门内走了几步，迎面拦下了克迪玛。

“您好克迪玛小姐。我是CTTI快递公司的服务员，有寄给罗斯科先生的快递，门卫先生说罗斯科先生不巧外出了，可您知道这种专程投递的快递是需要收件人签名的。您不要怪这位好心的门卫多嘴，他真是个好人，他告诉我您可以全权代表罗斯科先生收下这封快递。如果真是这样的话，我将万分感谢。您知道，最近的快递生意好得不得了，我可不想再跑一趟，当然了，在您方便签下芳名的前提下，我将不胜荣幸。”

看着克迪玛诧异的目光，苏珊一直僵硬地保持着微笑，手指却在收紧，攥成了一只拳头，她恨不得把拳头直接飞到这个女人的脸上，而从小就演技出色的苏珊还是很优雅地保持着淑女的笑意。当她拿着有克迪玛签名的单据拐过街角的时候，她忍不住想笑，想哭，想喊。

几经犹豫，克迪玛还是决定在罗斯科之前打开这个信封，看寄出地址，快递来自波兰。没听说他这家伙认识什么波兰的朋友。

里面只有一张贺卡。暗红的背景下印着满载礼物的圣诞老人和一只长

着犄角的鹿，卡通的画风显得多少有些幼稚和不伦不类。

“尊敬的罗斯科先生，感谢您的大力帮助，配方已安全抵达我处，相关费用将在第一批产品推向市场后的第一个月内全部转入您在瑞士的银行里。同时我处欢迎您在方便的时候，来风景如画的波兰做短暂停留，预祝您圣诞快乐。”

配方？最近公司上上下下都在对这个词过敏，原因就在于这个价值数亿的配方已被确认泄密了，流向何处未明。

波兰？会是波兰吗？克迪玛就近抓过一只电话听筒：“给我接FBI，国家安全局。”

接下来的一个月时间里，整个公司似乎平静了很多，罗斯科依然每天用那辆雪佛兰接送克迪玛，经常与公司高层领导一同出席各种重大宴会，依然每天签署为数众多的任免决定。直到FBI在波兰的市场上找到了第一批上市的配方产品之后，圣诞节过后不到半个月，这天上午，克迪玛的父亲面色沉重地拨通了罗斯科的电话：“我不知道应该叫你女婿还是别的什么，或者直呼罗斯科先生？对不起，这么早打扰你，我只是想知道，你什么时候在瑞士有一个银行户头的？”

苏珊终于可以开怀一笑了。罗斯科因盗窃、泄露重大商业机密罪被捕，加上苏珊全心全意地收集整理出的数以千计的非法电话入侵证据和由此造成的巨额经济损失，罗斯科面临至少十五年的监禁。

苏珊把母亲接过来，两个人在只够温饱的经济收入下，过着自给自足的生活。

这个真实的属于爱情的典型悲剧里，没有王子，也没有水晶鞋，有的只是罪恶、报复、丑陋的人性和坚强的求生欲望。苏珊的勇气在于把值得和舍得这两个词的真正意义，用一根电话线和一颗属于女性的易碎却又坚强的心，仔细地串在一起，成为黑客史上最著名的传奇。

【黑客知识】

BBS：英文全称是Bulletin Board System，中文“电子公告板”，其功能最早是用来公布股市价格等即时性信息的，它的出现给计算机爱好者提供了一个可以跨越空间距离即时交流信息的手段。在互联网初具规模的时候，最早出现的一种群体互动式的交流方式。在BBS可以把想说的话，想求助的事和急待解决的问题公布出来，由众多的浏览者给出答案，由于这是一种打破传统电话、信件限制的方便快捷的联络方式，使得BBS得以在世界范围内发展壮大起来，随后出现的功能更强大的BBS系统被称作论坛，现在广受欢迎的博客、微博等电子社区式的网络交流方式中，都可以找到最初BBS的影子。

1978年美国人开发出最早的一套BBS系统，称之为CBBS。1982年，Buss Lane为IBM个人计算机编写了一个原型程序，经过不断的运行和完善，发展成一个真正意义上的功能相对完备的BBS系统，这套被命名为RBBS-PC的系统拥有统一的界面和允许使用者自行设计和替换部件的能力，极大地方便了管理员对系统的维护工作，后来在开发其他的BBS系统时都以此为框架，所以RBBS-PC赢得了BBS鼻祖的美称。

最早的电脑使用者们经常会聚集在这里交流电脑的使用心得，渐渐的一些对电脑有着天然敏感的黑客们便把这里当做互换入侵技术的学习园地，早期的BBS其实并不是公开的可以随便出入的开放性空间。

米特尼克便在BBS上开发了一个需要凭借密码进入的私人空间，用来和他的黑客朋友们交换信息。

中国首例电话黑客案：2007年10月9日，武汉希望之星养殖技术有限公司在报上刊登了广告，并公布了公司的联系电话。就在第二天上午，该公司一位姓蔡的工作人员便接到一个奇怪的电话，对方声称如果蔡先生单位的电话遭到骚扰性攻击可以直接打电话给他，随后留下了一个手机号码。

蔡先生对这个电话感到莫名其妙，也不以为然，没想到仅仅隔了大约半个小时，公司接待室里的四部电话便此起彼伏地响个没完，接听后听筒里面只传来忙

音，来电显示屏上显示的号码是10个“0”。

焦头烂额的蔡先生这时候突然想到了那个奇怪的电话，随即按照记下的手机号码打回去，对方声称只要汇3000元给他就可以解决问题，同时留下了一个银行账号。

万般无奈之下这家公司只有报警。武汉市公安局东湖开发区民警赶到现场后，与当地的电信部门取得了联系，并要求电信部门以技术方式屏蔽掉对方的来电，而电信检修人员经过细致的检查之后表示，除了更换电话号码之外，也没有其他行之有效的解决办法，因为他们也查不出对方使用了什么手段来达成骚扰效果。

按照对方留下的手机号码，电信人员查到这个号码来自广州，但这个号码属于一个未记名的手机卡。

公安人员冒充公司的办公人员再次与机主取得了联系。在质疑对方是否有能力解决问题时，对方以十分钟为限，声称可以在十分钟之内阻止骚扰电话。

果然，在接下来的十多分钟时间里，办公室里的这几部电话都保持着静默，然后对方又拨回电话，“现在开始，我停止对这些骚扰电话的阻断。”话音未落，四部电话又争先恐后地响了起来。

公安人员再次联系了对方，并声称怀疑对方便是骚扰电话的制造者，当即被对方否认，对方称自己是一家网络安全公司，以他们的经验，每一个企业都会有自己的竞争对手，也都有可能以电话骚扰的方式被竞争对手干扰，为此这家安全公司就着重了解那些在媒体上公开了电话的企业，并提前向他们提供联系方式，一旦遭到类似的电话攻击，就可以主动服务，这是公司目前最主要的经营方式。

这回答似乎有理有据，但实在有点缺乏可信度，在公安人员表示怀疑之后，对方毫不客气地关掉了手机。而办公室里的电话，还在声嘶力竭地鸣响。

最后这家公司不得不重新更换了电话号码才算逃过一劫。

此案最终不了了之。

—— 第十二章 ——
穿越防火墙的独行侠

网络被称作‘第四媒体’，既然是媒体怎么能缺少观众和编辑呢？你们安分守己，那么你们就做个好观众，我呢？我来给你们爆料，给你们提供故事和随之而来的历险传奇。

——“剑客联盟”宣言

1 冰冷

如果你在1999年10月20日，格林尼治时间上午7点左右打开美国退伍军人事务总部的官方网站，你就会很新奇地发现，往日一本正经的网页被一行字修改得不伦不类：“真是过瘾。希望在被抓之前，我可以逃之夭夭。”

这戏剧性的一幕时间很短，网站的技术负责人在极短的时间里把首页恢复原状，好像什么事也没发生过一样，而事实上，有一个人确实来过，他小心翼翼地来，悄无声息地走，极其潇洒。

这个人绰号“冰冷”，一个躲在新西兰的英国人，一个自由战士，一个无政府主义者，一个技术精湛行事极其低调的黑客，一个乐观而豪爽的独行侠。

除了美国退伍军人事务总部的网站，这个号称“冰冷”的黑客不久前刚刚在软件业的龙头老大微软公司的网站上唱着歌走了一圈，他悄无声息地入侵了微软的会议管理服务器，成功地修改了其中的两个页面，在上面留下了自己的一句话：“冰冷到此一游，杀盖茨救世界。”

这一年，冰冷16岁。

入侵网络带来的刺激常让一些青年人热衷于其中并乐此不疲。这是一项需要年轻的冲劲和成熟的精湛技术相结合的事业，如果它可以称为事业的话。虽然很多人认为这很无耻，甚至很罪恶，但冒险的天性、巨大的挑战以及成功带来的喜悦和成就感，还是召至众多的精英级电脑高手为之奋斗痴迷不改，甚至迷恋到了在现实世界玩儿命的地步。他们其中的很多人目的很明确：为了钱。而更多的人则只为了一时痛快，为了考验自己的技术，他们来无影去无踪，在网络世界里叱咤风云。对他们而言，“黑客”这个名词本身就是一种至高无上的荣耀和奖赏。

冰冷无疑是其中的佼佼者。在他的带领下，“剑手联盟”盛极之时有200多人。他们群策群力，向着代表垄断的那些行业巨头的网站展开一轮又一轮疯狂地攻击，他们的宗旨是“电脑软件及其中所包含的技术应该免费共享，所有在这两方面获得利益的人都是电脑界的败类，也都应该成为人人喊打的丧家犬”。

“剑手联盟”是一支敢啃硬骨头的队伍，他们专门打击软件业的领军人物和社会福利机构中的收费部门，除了微软，甚至包括SUN公司等世界级的大公司网站都有他们的影子幽灵般的出现。在杀毒软件方兴未艾时，这些冰冷的剑客们纷纷剑指杀毒软件公司，对着那些号称无一漏杀的杀毒软件发起挑战并屡获成功，他们每一次出场都赢得黑客圈的掌声雷动。

病毒在线是一家服务器位于美国西海岸的杀毒软件公司，其当家产品是在线杀毒，很多中了病毒的电脑不需要下载软件，只要登录这家网站的首页并注册成功，就可以免费得到这家网站的救助。在网站开放初期，凭借着“免费杀毒”的金字招牌，这家网站的日点击量保持在100万左右，

如此巨大的点击量给这家网站带来了丰厚的利润：杀毒是免费的，但每个来网站免费杀毒的用户都会发现，网站的首页上广告越来越多。

在网站开放四个月后，那些尝到了免费杀毒甜头的用户们突然发现，网站虽然还可以访问，但却莫名其妙地变为了只能查毒不能杀毒。网站的声明称今后本站只提供查毒，如果用户感觉自己的电脑中了病毒，可以在本网站上免费使用查毒功能，若是想彻底杀掉病毒，请重新注册为付费用户。

这一更改引起了用户的强烈不满，虽然免费查毒在当时也是绝无仅有的，但习惯了免费杀毒的用户们都有一种被骗的感觉：网页上夹杂了太多的广告，在骗取了用户的无数次点击之后，突然把最主要的服务改为收费。这种经营模式的突然转变，引起用户的极大不满。

一个月黑风高的夜晚，冰冷的剑客们出手了。

冰冷派出的高手先是在一个位于俄罗斯的IP代理服务器上隐藏了真实的IP地址，然后成功地绕过了网站的防火墙，在一个不易察觉的系统漏洞掩护下悄悄地在系统内部植入了一个跟踪程序。随着跟踪程序的启动，当用户点击这个网站的首页时，就会启动由跟踪程序修改的一小段代码，而这段代码则将网站首页的所有链接都引向另一个黑客新建的页面上去。在那个页面上，空无一物的黑暗中会渐渐显露出一个由程序自动计算并绘制的猫眼动画，这个猫眼每眨一次就会挤出一个字母，最后会构成如下一句话：“世界上最正统的骗子之一——病毒在线。的确，所有的病毒都在这条线上。这是一条死亡之线，一个无耻的骗子，一个低级的下流团体和道德缺失者的集中营。”

“剑手联盟”显然是和这家公司较上了劲，病毒在线只要一修复网站，“剑手联盟”就会在第一时间重新修改其首页链接，使得每个来访的用户都有机会目睹一段猫眼动画并大呼过瘾。病毒在线在升级了底层系统之后重新加装了更为严密的防火墙，但所有这些在高超的、有备而来且坚持不懈的“剑手联盟”的攻击下都无济于事，直到病毒在线把系统内核由微软的NT操作系统改为苹果系统之后，重新设计了网站的核心源代码，

“剑手联盟”的攻击才有所缓解。到最后，病毒在线显然失去了信心，由于公司错误地把免费杀毒变为免费查毒，网站的访问量急剧下降，再加上“剑手联盟”不间断的持续攻击让这家公司焦头烂额，虽然最终降低了对手的攻击成功率，但网站还是经常被改得面目全非。病毒在线在苦苦支撑了六个月之后，被另一家实力雄厚的大企业收购，由免费查毒改为一个病毒破坏性测试网站。到此为止，“剑手联盟”的攻击才宣告彻底停止。

在与病毒在线的龙虎斗中，似乎以黑客身份出场的“剑手联盟”并不光彩，但这一场网络战却打得十分精彩，冰冷也由一个16岁的孩子长大成一个需要承担法律责任的成年人，而这对冰冷来说却并非是一件令他感到愉快的事情。在他又一次入侵一个位于德黑兰的军用计算机系统时，聪明的管理员锁定了他的位置，并在国际刑警的协同下，把远在新西兰的冰冷成功捕获。

冰冷在警察突然出现之后表现出黑客惯有的冷静。“看到桌上的咖啡了吗？那是我的晚餐，我可以把它喝掉吗？”在得到警察的首肯后，他仔细地、一滴不剩地喝光了咖啡，然后很平静地问：“我们要走多远？我需要带上我的护照吗？”

冰冷将面临最多七项指控，而法官对这个自喻经常手持正义之剑出现的侠客级人物显然心存好感，最后只象征性地惩戒了这个年轻人。被判一年徒刑、缓刑三年的冰冷目前仍然可以每天咬着面包，兴高采烈地面对着他的武器——那台配置不高的、启动后如风箱般作响的旧电脑。在他手里，任何一台配备了键盘和显示器的电脑，都是一件代表着正义的无坚不摧的攻城利器，也正是电脑让这个年轻人成为一代黑客的榜样之一。

❷ 左肩

1987年夏天，夏威夷的海滨公路上发生了一起离奇的交通事故。说它

离奇，倒不是事故本身多新鲜另类，而是处理事故的交警在那辆肇事逃逸的车上找到了车辆行驶证，按照行驶证显示的数据，这辆车属于一个叫凯德撒姆的人。

叫凯德撒姆的人并不多，而交警有个同事，正好就叫这个名字。交警在登入车辆管理系统后发现，这辆车的车主真的就是自己的同事。按照惯例，他输入了同事的行驶证号，在与之对应的车主信息中，自己同事的照片居然是一个长头发的女人。

随后的深入调查中，交警部门把这辆奇怪的车大卸八块，最终在车架上找到了出厂号牌。号牌上的信息表明，这辆车的真实车主是一个叫罗宾的白人，相关信息表明，罗宾的职业是一家电信公司的网络管理人员，他现在正请了长假，在夏威夷度蜜月。

接下来找到罗宾就变得容易很多了，罗宾显然也没兴趣和警察玩躲猫猫的游戏。在警局里罗宾很配合，他承认自己酒驾并肇事逃逸，心服口服地接受处罚。当警察问及车主照片一事时，罗宾显然有些准备不足，作为一名黑客，他做过的修改当局数据资料库的事情太多了，这件事显然早被他忘得一干二净。

罗宾开始皱眉。他显然已经意识到，这已经不是一起简单的交通肇事案件了。

随后对罗宾的深入调查中，当局惊讶地发现罗宾的电脑里除了最简单的文字处理软件外，竟然安装有多达140多个网络跟踪入侵软件，从最简单的IP轰炸工具到最复杂的伪装木马编辑器，面面俱到不一而足，警察甚至发现了一份记载着罗宾入侵各大重要网站的时间、地点以及详细的攻击过程的电子文档。在一般黑客的眼里，掌握了这本攻击记录，无疑就是得到了一本极具实战指导意义的黑客入侵百科全书。警察惊讶地发现，这个皮肤白皙的年轻人，居然就是大名鼎鼎的当局悬赏32万美元追捕的超级黑客“左肩”。

在黑客圈子里，提到左肩，算得上是众人皆知。这个堪称传奇的神秘

人物一向独来独往、行踪诡秘，他像吸食毒品一样痴迷于黑客入侵，如其他黑客中的高手一样，随意进出各种高端机密网站及后台数据库，到处横冲直撞。

左肩的目标只锁定那些是国家最高机密的国防、军事和银行等网站。奇怪的是，他并不把那些到手的机密拿出去换钱，事实上随便哪一份有关美国核弹的分布图都可以卖到上千万美元，而左肩只是把原始数据复制之后将现有数据进行修改，然后留下说明告之管理员正确的数据被存放到什么位置，最后署下自己的大名就悄然退出。他放弃了这些价值数亿的机密数据，每天在自己任职的公司里做着最枯燥的工作，拿微不足道的薪水。

“正如你们所知，只要我想，我随时可以成为亿万富翁。但黑客的精神告诉我，钱不是最重要的，重要的是胜利，是获胜的过程。”左肩平静地像是在讲述别人的故事。“这世界上，能真正给我满足感的，就是迎接挑战，并赢得挑战。钱够用就好，而且你们应该相信，只要我想，钱对我来说只是数字而已。”

没有人认为他在说大话。无数的事实证明，他一夜之间就可以从一文不名的小职员摇身一变成为身价过亿的巨富，但谁又能否认，黑客这个名词本身就预示着，从事这一职业的人都或多或少地有着常人不可理解的怪异性格呢?

左肩第一次黑客入侵试验始于中学时代。那个时候计算机还不普及，老师每次都要他们先去打扫操场，直到整个操场看不到一片落叶和纸屑之后才允许他们上机20分钟，这让那些对计算机充满好奇心的年轻人怒不可遏。当时家境相对比较宽裕的左肩于是央求父亲给他买了一台计算机，仅仅三个月之后，他就发现自己对计算机编程有着天然的领悟力。在试着做过几个小程序之后，他开始留意学校机房里那个用绞线连接起来的局域网系统。

再一次的计算机课上，当老师安排他们去打扫操场的时候，左肩偷偷地溜回教室，快速地在计算机中插入一张软盘，把自己用了两个晚上编写

的一小段程序在局域网上运行起来，仅仅几秒钟系统就把管理员的密码以明文的方式反馈给他，随后他修改了这个密码，然后悄悄地溜回到操场。再上机的时候，看着老师不断地输入密码，茫然地望着“密码错误，请重新输入”的对话框紧锁眉头时，恶作剧的成功让这个年轻人很是得意。

从那一刻起，左肩疯狂地爱上了黑客这个身份。

他中学只读了一年就辍学在家，躲在小阁楼上每天至少把20个小时花费在电脑上。他编写的程序简单实用，16岁时他就成功地卖出了自己的第一个软件作品——一个超市综合管理系统，并得到了400美元。这笔钱拿到手后，他立即给自己换了一台新电脑，并安装了调制解调器，每天在它吱吱呀呀的嘶叫声中在网络世界里探求。

他本来可以在程序员的行业里做到最出色，但是程序员平稳呆板的生活状态，显然无法让他再次体验那种电流穿身的快感和喜悦。他每天最想做的就是把那些“*”号代表的密码一探究竟，这个欲望不断膨胀的结果就是，他疯狂地迷恋着“黑客”这个名词能带给他的全身心的快感。

17岁那年的夏天，他无意中破解了FBI设在西海岸分部之一的主页面后台系统密码。以管理员的身份在系统中逛了一圈之后，他发现真正的管理员也在线，于是他好意地与管理员搭上了话，并告之他们的系统存在安全漏洞，聊了几句之后管理员发现这只是个毛头小伙，于是极不耐烦地把他踢出了系统。当他过了几天再次来到这个网站，发现管理员并没有拿他的警告当回事，系统还是存在着漏洞。这一次，他决定给对方上一课。

左肩修改了这个网站的系统主页面，使每个登录网站的浏览者都被拉到某个免费视频网站上去看电影，并一举攻破了管理员账户，把所有的管理员权限都降为普通注册用户，系统中只留了自己一个超级管理员。

最后这个FBI分部的网站系统不得不重新升级到严密级，为此他们花费了大约两周的时间。在这两周的时间里，左肩可以随意修改页面，或贴上一个笑话，或画几个好玩的卡通画。看着管理员每天狼狈不堪地修改网站，左肩拍腿大笑，并发现那些貌似固若金汤的系统也不像他们自己宣称

的那样无懈可击，只要自己留心，还是有机可乘的。

从此他把所有的时间都花费到寻找那些高机密网站的系统漏洞上，并在每一个可以入侵的网站上留言，声称发现了漏洞。“你只需要付5美元，我帮你处理好，这价钱我相信是有别于敲诈勒索并极其公道的。”

但是没有一个人认为这个不足20岁的小伙子有如此的通天本领，几乎所有人都对他的警告不予理睬。

被人忽视和看低是每个年轻人都不能容忍的。左肩开始修改这些已经掌握了管理权的网站中的文件，但他的底线是善意提醒，并不会故意弄丢网站的数据，也不随意删除用户，只是把一些有趣的东西植入系统之中，或是一个猜拳游戏，或是把一些文件加上简单的密码放到别处，“你们完全可以像我一样，猜猜密码是什么——实际上这很好玩。”

很多杀毒软件和网络防火墙的开发商都对左肩无可奈何，生怕哪天左肩兴致所至找上门来，因为这种以计算机安全为主打产品的厂商最怕的就是自己的网站被黑，这就像一个优秀的警察在自己的办公桌上发现了自己家被盗的案件报告，对产品的形象打击最大也最直接。不幸的是，显然那些视左肩为无能小卒的人极大地刺激了这个超级黑客的报复心，只要是左肩感兴趣的地方，无论防卫多么严密他似乎都能为所欲为，没有什么能真正抵挡得住左肩的脚步。每一次入侵，他都会精心准备，先以普通浏览者的身份多次打探虚实，在感觉有把握入侵的前提下，他就会把自己的IP地址巧妙地指向系统防火墙的绝对路径，最大限度地接近防火墙而不引起系统的怀疑。形象一点的说法是，对方挖了一条极宽的正面战壕，而自己则努力绕过战壕，从侧面进入战壕后面的薄弱地带展开攻击，因为一般的系统多是以防火墙软件为唯一的屏障，最多是多设几道防火墙而已，只要找到了防火墙的薄弱环节，其他的事自然水到渠成。

就像魔术一样，看起来神秘莫测，其实说穿了都很简单，只是实现过程完美与否的问题。左肩的每一次攻击都堪称典范，他通常会同时启用两台计算机：一台用来破译密码、绕过防火墙从而进入系统的核心区域；另

一台则以普通用户身份登录系统，再通过挂接特殊的软件来侦测是否有管理员或是网络安全人员接近自己，侦查与反侦查同步进行。在得手之后，先关闭主攻击电脑，然后在另一台电脑上以管理员的身份逐步清除掉自己的作案痕迹，然后全身而退。这一切做得滴水不漏，故而他虽然进出各大安全系数极高的网站并留下自己的名字，但他真正的身份和上网痕迹却很难留在犯罪现场。在如此完美谨慎地自我保护下，左肩在成功地入侵了大约400家顶极知名度的网站后仍能逍遥法外，而国家安全局及相关部门则对这个不速之客知之甚少，虽然32万美金的悬赏通告发布已久，但仍然毫无线索，倒是那个幸运的交通警察歪打正着地将左肩绳之以法。

那巨额的奖金，足够一个交警安稳地过完他的后半生了，只是不知道，他最后是不是很有风度地向左肩致谢，感谢他给了自己一个发财的机会。

❸ 卷刃刀

服务器位于新泽西的“过关斩星”网，一度是最热门的黑客聚集地，网站奇特的运营方式吸引了大批黑客云集此处，老手们在这里一展才华，新手们则把这里当作一个学习交流的圣地。这个纯娱乐性的网站每周举办一次黑客大赛，每月的4位周冠军在月末时进行月赛，12位月赛冠军则参加年度总决赛，年赛获胜者将被冠以星级大师的称号。虽然这项比赛没有奖金，但实际上又有几个黑客真的是因为盯上了金钱而痴迷其中的呢？那种获胜后的满足感才是至关重要的。

比赛通常是以选择题的方式进行，在每一道题中都或多或少地给出一些提示，要求比赛者或进入某一网页进行密码探听，或在一个长长的句子里找出规律，其答案最终都转化为一个数字，按这个数字标明的题号进入另一道题重新选择，一旦错误就失去比赛资格，也就是说，答题者必须保证每道题都找到正确答案才有可能过关斩将成为冠军。

这种疯狂的游戏吸引了世界上众多的著名黑客光临现场，甚至包括大名鼎鼎的凯文·米特尼克和柏森这些重量级的选手，而很多国家的计算机网络安全专员也混迹其中，试图从中打探出某些有前科黑客的踪迹。

2001年的星级大师终级赛上，一路过关斩将的12位选手，到最后仅剩3人，要回答的问题也只剩6个。

除了参赛选手的忙碌，很多局外人也在忙，其中包括美国FBI的网络安全专员查尔·哈德克。

吸引哈德克注意的是一个网名“卷刃刀”的黑客。种种迹象表明，这个自称生在德黑兰的犹太籍黑客，就是当局悬赏15万美元的入侵韩国国家机要总局和美国陆军驻韩国特种部队网络工程中心，并窃取了美国在中东及东亚的防御部署和未来15个月中武力集结命令的原“狼烟”黑客组织的领袖人物卜卜西洛，一个有着中亚血统的美国人。

卜卜西洛把这些窃取的情报以天文数字般的价格卖给了克格勃的相关部门，并已承担起克格勃在东亚地区的军事网络监听刺探工作，是一个俄罗斯雇佣的职业军事黑客。因其目前具有美国国籍，他已涉嫌包括泄露军事机密、非法入侵国家军用设施、贩卖国家高等秘密等七项指控，如果被捕，他将面临的是最高25年的监禁和数额巨大的罚款。为此，当局悬赏15万美元，并为这个高度危险人物专门设立了跟踪档案，专人负责，一有机会便可以实施抓捕。

作为FBI网络安全精英之一的哈德克，在美国国家网络安全办公室做了6年极其悠闲的专家顾问团成员之后，终于耐不住性子把自己下放到技术最前沿和网络“战斗”的第一线。一生致力于反黑行动的哈德克和他随时要面对的黑客一样，是个无法让自己安定下来的狂热分子，他的血液里天然地涌动着一股冲动的因子，卜卜西洛就是他的最新目标。虽然在抓捕德国籍黑客教父卡布哈奇的行动中他居功至伟，但那一次毕竟是多兵种合作，而这一次他发誓要单枪匹马，生擒卜卜西洛，为他即将引退的职业反黑生涯画上一个最圆满的句号。

他已经跟踪卜卜西洛长达6个月之久，后者最后一次职业军事盗窃任务是，成功地把日本驻美国大使馆有关韩朝双方秘密磋商的正式备忘录全文交给俄罗斯国家军情分析研究所，而这份备忘录的安全等级为橙色，仅次于最高级的红色。

就在这次盗窃中，哈德克终于捕捉到一个看似真实的后门入侵程序的残片，这个程序显然是卜卜西洛在退出系统时不小心遗留下来的：他没有完全把程序运行的临时文件清理干净。而哈德克就是在这近200个临时文件中，搜寻出一个编制程序时的习惯动作，系统留下的“卜卜西洛，2001年3月编写于中国云南”这一行文字，并且在这些蛛丝马迹中，卜卜西洛似乎还暴露了一个真实的IP地址，经查果然属于中国云南某市，看来在把中国云南某市的旅馆、饭店翻个底儿朝天之后，一定会有些收获。

于是哈德克便持一张旅游签证，以一身牛仔裤、旅游鞋的装束来到了云南。

3个月时间过去了，哈德克和助手在云南某市相关部门的帮助下走遍了全市数百家卜卜西洛可能的藏身之地，结果一无所获。就在这时，他的助手从美国的实验室发来信息，卜卜西洛很可能参加了“过关斩星”网的黑客比赛并成功入围年度总决赛。

接到这个消息时，哈德克正在石林风景区做一名真正的游客。云南是中国的旅游胜地，虽然他此行的目的并非游山玩水，但已入宝山自然不能空手而归，到了云南不游石林显然就如同到了巴黎而不去看一眼埃菲尔铁塔一样遗憾。

哈德克早就吩咐自己的助手们留意这个各方“神圣”云集的黑客大赛网站，因为以他的经验推测，没有哪一个黑客能回避这种可以在大庭广众之下一展身手的好机会。黑客行径都是暗无天日的，而这样一种可以把才华在天底下所有黑客面前一一展现的机会，是每个黑客都急切盼望着的。他坚信在时间允许的前提下，黑客领域的大哥级人物卜卜西洛也一定不会错过这样的机会。如果助手传来的这条信息属实的话，只要把这次大赛目

前仍然未被淘汰的几位选手的相关数据做一个仔细的分析，就不难发现卜卜西洛的藏身之地，这总好过自己在偌大的云南大海捞针。

哈德克立即把所有的跟踪信息都指向了此次参赛的黑客选手。他的实验室里7位冲劲十足、技术精湛的助手也全力以赴地扑到赛场上，他们和选手们一起做题，争取最先得到正确答案然后在答案指向的某一个网页上抢先植入木马跟踪程序，待选手们选中答案也进入到这一网页上时，跟踪程序开始抽丝剥茧般地分析选手们的各种网络信息，包括计算机系统的位置和正确IP。要知道黑客们最讨厌的就是自己的真实IP被暴露在光天化日之下，所以几乎每一个黑客在上网的同时都要挂上代理IP服务器，把自己的物理IP指向一个虚拟的网络服务器，这样就给自己起到了极好的保护作用，只有自己攻击别人的份，别人无法查到自己的真实地址，从而使所有针对自己的网络攻击陷入失去目标的尴尬境地。

就在哈德克和他的助手们进入到赛程设定的某个页面时，却遗憾地发现该页面已被改得面目全非，原有网页的内容全部被删除，只留下一行嚣张的文字：“卷刃刀来过，他带走了正确的网页信息，下一站，只有他一个人知道。哈德克，您还是稍逊一筹。”

就比赛的结果来看，卜卜西洛果然技高一筹，他最终摘得了“过关斩星”网站的年度最高大奖，赢得了星级大师称号，而哈德克和他的助手们，这一次无疑又遭遇了最彻底的失败。

星级大师卷刃刀，也就是我们的主角儿卜卜西洛，最终仍像一条见首不见尾的神龙般成功地躲避了追击，潇洒地游走在网络的江湖之中，而他本人则更喜欢被人称做“佐罗”，那个蒙着面孔，偶露端倪的正义化身。

【黑客知识】

SUN公司：1982年，Sun Microsystems公司诞生于美国最著名的斯坦福

大学，其经营理念为“网络服务于所有计算机，并为之打开方便之门。”它是世界上最大的UNIX系统供应商。并以其高度灵活性、简约性、可靠性和可用性等指标赢得全球各个行业客户的青睐。

IP代理服务：每一个上网用户都必须有一个自身在网络中的标识，这个具有唯一性的网络标识就是IP，其功能类似于现实生活中的门牌号，所有向网络发出的请求都会从这个IP地址发出，并成为网络信息的最终返回地址，因为IP地址会被一些有特殊功能的网站或程序记录下来，那些不想被人发现自己IP地址的计算机用户便会寻求一种隐藏或改变自身IP的方法，于是IP代理服务器应运而生。其功能就是代理网络用户去取得网络信息。或者说，代理服务器是介于浏览器和Web服务器之间的一台服务器，有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。这样记录在目标网址上的IP浏览记录就会被显示为IP代理服务器的IP地址，从而成功地隐藏了浏览者的真实IP地址。

黑客经常用这种方法来进行自身隐藏，从而达到欺骗追踪者的目的。很多正规软件也支持代理服务器，比如最常用的IE浏览器和国内使用者众多的QQ网络通信软件，都可以挂载到IP代理服务器上运行。

IP轰炸工具及常用的黑客攻击方式：黑客攻击手段可分为非破坏性攻击（善意）和破坏性攻击（恶意）两类。非破坏性攻击并不盗窃系统资料，而更接近于一种游戏和调侃式的玩耍，主要面对个人计算机用户；破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的。

后门程序：目前集体合作性质的大型软件的编制都是模块化组合设计的，将整个项目分割为若干个模块，由不同的编程人员分别进行设计，在设计成功之后再合成为一个大型的软件系统。软件在开发阶段通常会人为地设计一些后门，便于后期测试和改进程序，在软件研制成功之后，这些后门便通常会被封堵，从而使软件具有最高的安全性，但有时为了推出软件的更新版本或是程序员人为等因素，这些软件后门并没有全部“关闭”，从而成为黑客们进行网络攻击的跳板和媒介，黑客们在面对防火墙或一些具有网络存取功能的软件时会利用穷举法搜索

并利用软件可能存在的后门，然后进入系统并发动攻击。

信息炸弹：网络服务器上存储着大量的信息供浏览者使用，每个浏览者登录网站都会占用其一个信息通路，而一个网站的信息通路是有限的，信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，从而占满网络服务器信息通路，使正常的使用者无法登录网站，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。

拒绝服务：又叫分布式D.O.S攻击，与信息炸弹的攻击方式类似，但威力更大。信息炸弹只是由零散的黑客发出，而拒绝服务则是先侵入并控制某个网站，然后在网站服务器上启动一个控制进程，攻击者把攻击对象的IP地址作为指令下达给进程的时候，这些进程就开始利用网站超大规模的吞吐量对目标主机发起猛烈的信息炸弹式攻击。与信息炸弹相比，这种攻击方式可以集中利用大量的网络服务器带宽，对某个特定目标实施覆盖式攻击，因而破坏力超强，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。

—— 第十三章 ——

战争从网络迈向前台

胜利者是不鼓掌的，鼓掌的只是那些看热闹的观众。

——陈盈豪

1998年7月26日，美国加州，多云天气，微风缠绵。

威尔迪拜与往常一样，在上午和煦的阳光下打开计算机，接上网络，进行他每天开机后的第一件事：收发邮件。他的业务关系和与客户之间的信息传递大多是通过电子邮件完成的。

处理完邮件，他开始准备将新增的客户订单存入Excel文档以进行归纳和整理。但就在这时，他忽然感觉自己的机器有些异样。主机上的硬盘指示灯长亮不已，系统运行变得缓慢，鼠标指针和文字输入也变得异常迟钝。硬盘指示灯长亮说明硬盘正在全速读写数据，而鼠标指针和键盘输入的反应缓慢也说明系统正在进行复杂的计算，而他只不过是打开了Excel软件而已，并没有什么需要系统复杂运算的操作。

“希尔，快来看！我的电脑好像死机了。”他大声地叫着厨房里准备早餐的妻子。希尔是个计算机文员，对计算机的相关知识的掌握和操作水平都要比半路出家的丈夫要好很多。

希尔等待了大约5分钟，系统仍然没有好转的迹象，硬盘指示灯还在不停地闪烁，主机中的硬盘疯狂地旋转并声嘶力竭地发出一种持续不断的

轻响，似乎要在旋转中破碎一样。在确信了没有特别重要的数据需要存入硬盘之后，希尔无奈地将主机电源强行断开。“也许这只是一只Bug[①]在作怪，重启一下也许就没事了。”说完这句话，希尔若无其事地重新回到厨房里，把全部的精力都集中到一盘看上去让人胃口大开的蔬菜沙拉上。不过片刻之后，她便胃口全无。电脑前的丈夫又一次喊了她的名字，声音显得很无助：“亲爱的，再过来一下好吗？我的电脑……我的电脑，它好像病了，而且，病得不轻。”希尔摇摇头。丈夫总是大惊小怪，把责任推到电脑身上而不承认他自己是个电脑菜鸟。

再一次来到电脑前，希尔发现计算机没有像往常一样进入“蓝天白云”背景的Windows登录界面，而是停留在自检程序处，黑底白字地不动了，只有一个光标在一连串的英文字母后寂寞地闪动着。也许是硬件错误，希尔这样宽慰着自己，伸手按下了电脑的“重启”按钮。

正常启动状态下，电源接通后电脑会以短促的“滴”声来提示计算机硬件启动正常，而这次启动却没有听到那熟悉的声音，甚至连光标和自检画面的英文都没有了。除了电源风扇在正常旋转以外，整个计算机没有任何反应，显示器的电源指示灯一直处于黄色的通电而未收到主机信号的状态，而正常启动数秒后这个指示灯会由黄变绿。

一切症状表明，计算机很有可能发生了硬件故障。希尔找来改锥，把主机箱打开，将内存、显卡、硬盘等各种硬件设备和连线重新插牢，在确认没有硬件接触不良之后，再一次按下电源键，电脑依然毫无反应，丝毫没有正常运转的迹象。

是哪个硬件出现了故障吗？无奈之下希尔拨通了电脑公司的维修热线。让她惊异的是，电脑公司告诉她，今天早上，公司已经接到了数十起这样看似硬件故障的无法启动的机器维修任务。

“这个世界要陷入一场灾难了吗？”

① Bug：意为系统的小错误，或是程序运行时遇到的故障或本身存在的小漏洞，这种系统错误在Windows9X时代经常出现。

❶ 史上最强病毒

被希尔不幸言中，这个世界从这一天起，真的开始了一场空前的灾难，而且造成这场灾难的元凶是一小段程序代码。这段由数字和字母组成的代码以几何级的速度在整个互联网上铺天盖地地肆虐开来，如同一场瘟疫，在极短的时间里就在全球范围内造成了无法估算的巨额损失，而这灾难的受害者，正是那些由硅元素、塑料和金属组合而成的电脑。一个在当时风靡一时的电脑游戏在推出的Demo[①]光盘中竟然携带有这种致命的计算机病毒。于是，这种病毒凭借这种发行量达几十万份的光盘拷贝迅速在美国各地传播开来，业界惊呼，全民惊恐，染毒电脑呈指数上升。

所有发生疑似硬件故障的电脑基本上有两个共同的特征。一是某些型号的主板BIOS被恶意篡改和烧毁。BIOS即电脑中的“基本输入/输出系统”，存放的是系统最基本的硬件参数和驱动程序，一旦被破坏，系统则根本无法启动，唯一的修复途径就是送回厂家重新装载BIOS程序；另一共同特征便是计算机的硬盘从主引导区开始，直到硬盘的最后一个分扇区全部被垃圾数据填满，所有保存在硬盘中的数据被破坏性覆盖。很多银行，甚至美国中央情报局等重要部门的计算机同样未能幸免，中毒后的计算机是真正的“死”机。

美国国家计算机安全中心立即对这一普遍存在的突发故障进行最高级别的技术分析。通过对用户硬盘数据的技术检测，所有能读取数据的硬盘中都查出了一种标识有CIH的数据文件，也许正是这种带有CIH标识的文件使得计算机的BIOS信息以及硬盘数据丢失，并由此造成大批的计算机陷入瘫痪。

进一步的技术分析肯定了这一最初的判断，这种带有CIH标识的文件

① Demo：展示版，试玩版。计算机软件行业术语。歌手在推出新的唱片时也会事先给唱片公司送去Demo碟，以展示新歌。

是一种新型的病毒程序，它有若干不同的版本，有的破坏计算机的BIOS，有的则向计算机的硬盘中疯狂写入无效数据，致使用户的计算机数据全部丢失而根本无法通过技术手段进行恢复。最恐怖的是，以往的计算机病毒只能破坏系统的软件数据，对硬件则无能为力，这样在做好系统重要数据的备份之后，可以简单地通过重新安装操作系统来恢复计算机的功能；而这种新生的病毒居然可以对某些型号的计算机主板系统进行破坏，用无用数据覆盖掉主板BIOS，使得计算机无法正常启动，而BIOS中的数据只能通过计算机厂家重新用专用工具加载正确的数据后，才能使主板重新正常工作。这种修复，普通计算机用户是无法在自己的办公桌上完成的，这标明CIH病毒已具备了对硬件的彻底破坏能力，它可以从最根基的地方摧毁计算机，从而使计算机陷入彻底瘫痪。

一个月后，这种恐怖的如幽灵般的计算机病毒现身中国。1998年8月的最后一天，中国公安部发出防范CIH病毒的紧急通知，要求拥有银行、公安等国家机密和重要信息存取权的计算机，一定要做好数据的备份工作，同时严格禁止使用来源不明的各种光盘、软盘以及来源于网络的程序等。新华社、中央台新闻联播栏目多次全文播发该公告，对中国计算机用户进行全方位的预警。但国内仍然有计算机终端不断感染这种新的病毒，一位老军人耗费多年心血写下的30余万字的回忆录在电脑中顷刻之间丧失殆尽；众多公司的客户资料等也在计算机中化为乌有，很多电脑昨天还完全正常，今天就无法启动，之后便信息丢失、数据被毁。计算机维修公司和主板生产厂商也都忙于BIOS的修复工作，而很多计算机公司在很长一段时间里接不到一宗购买电脑的订单，很多购机者害怕刚从商店搬回家的电脑很快就会变成一个不声不响的废物。一时间世界各地谈“毒”色变，很多存储有重要数据的电脑在正常关闭之后便不敢再启动，因为担心数据插翅而飞，“在没有安全的病毒查杀方法出现之前，让那些数据先老老实实地待在硬盘里总比一下子全部被毁要好。”许多公司只能看着关机后的电脑默默发呆，而电脑旁边则围着众多一筹莫展的客户。

中国各大报纸和新闻媒体也不惜版面，在显著位置刊发大量CIH来袭的报道，一时间几乎全球的计算机用户都陷入一种人人自危的状态中，在随后的几年时间里，CIH如洪水猛兽般地席卷了计算机世界。

据非官方公布的数据显示，1999年3月，在IBM 的Aptiva 计算机系统中发现恶意预装的CIH病毒，很多购机用户第一次开机就惨遭黑屏；1999年4月26日改进版的CIH首次在全球大范围爆发，超过6000万台电脑被不同程度破坏，全球损失超过20亿美元；2001年4月26日CIH 第三次大发淫威，仅中国北京当天就有超过6000台电脑遭CIH破坏，当天报修硬盘数量接近400块。但因CIH病毒一旦发作计算机硬件就算基本被毁，硬盘数据几乎全部消失，加之病毒编写者不断地改进病毒程序，使之破坏力更大，病毒潜伏时特征极不明显，而一旦发作便是毁灭性的打击，能够捕捉到病毒源码的概率非常小，查找和抵御病毒的难度非常大。

从第一例感染CIH的计算机开始，已经过了数月之久，病毒在长时间里造成了巨额损失后仍然不能被查杀，几乎所有的杀毒软件都对其工作原理和病毒特征知之甚少，只发现了一个规律，就是这个病毒只在每年的4月26日发作，少数变异病毒每个月的26日发作。因此很多不得不天天使用电脑的用户，每天开机所做的第一件事便是修改系统时间，使电脑的系统时间避开26日。这个笨办法很有效，对于一般用户，即使感染了，但因时间不对，病毒继续保持潜伏状态。而对于银行等对日期的准确性有严格要求的计算机用户，这一办法则行不通，这对一些经常鼓吹反病毒能力超强，并让用户付出大把钞票购买防御软件的反计算机病毒的公司而言，则更为棘手。各界民众也对反病毒厂商的不作为感到愤慨，其实这些厂商也是无法作为，包括美国计算机安全协会在内的各大政府机构也强硬地要求这些厂商尽快发布行之有效的对抗办法和杀毒软件，以改变这种被动局面。这些面上无光的反病毒厂商则不约而同地联合在一起，彼此交换信息、商量对策，以往对自家核心技术严格保密的杀毒软件公司这一次也开诚布公，目的只有一个，那就是把CIH斩于马下，使世界从这个自电脑出

现以来影响最大、传播最快、破坏力最强的顽疾手中解脱出来。

❷ 陈盈豪和他的CIH

“根据初步跟踪分析，CIH病毒是从海外传入内地的。”北京冠群金辰软件有限公司反病毒专家王铁肩介绍说。CIH病毒最基本版本加改进版共计五种，它们的相互区别在于基本版会使受感染文件增长，但不具破坏力；而改进版则不增长受感染文件的长度，但具有摧毁硬件的能力，它们的发作时间分别为4月26日，6月26日和每月的26日。因为使用了VXD技术，这种病毒只对Windows95/98有效。

1998年年底，经过各方的不懈努力，终于相继出台了针对CIH病毒的查杀工具，这些仓促之间发布的查杀工具虽然不能完全抵御病毒的肆虐，却可以对已知版本的病毒进行预防并使其破坏力大大降低。在国内，CIH的疯狂也成就了一家原本默默无闻的反病毒公司，那就是冠群金辰公司，由这家公司出品的KILL98认证版杀毒软件是国内首家比较完善地能够查杀CIH的软件。一时间KILL98遭到疯狂抢购，而为了尽早买到一套KILL98，很多计算机用户不得不半夜起床到销售点去排队等候，随后国内老牌的杀毒软件厂商如江民、瑞星等，也相继推出了可以查杀CIH的反病毒软件。CIH的强大破坏力终于得到了抑制，一场病毒与反病毒之间的激烈对抗渐渐趋于尾声。

随着对病毒源代码的不断深入分析，和对病毒制作者遗留在病毒源代码中各种信息的追踪，以及病毒发作日期之一与苏联切尔诺贝利核电站事故同为4月26日这一天的线索，调查人员最初推测这很可能是民间某个对核能应用感到愤慨的和平人士进行的一场反核声讨，随后的进一步调查推翻了这一观点。最后通过不断努力和各种病毒信息的汇总分析，人们发现这种超级强悍的病毒最早出现在中国台湾，于是将所有的注意力都对准了那

个不算大的小岛，那个经济迅猛发展，人称亚洲四小龙之一的中国台湾。

1999年，CIH病毒的始作俑者陈盈豪终于落网。随后的法律调查中，这个超级病毒制作者的文弱和偏激让办案人员们大吃一惊。

陈盈豪，1975年出生，是个刚刚毕业开始服兵役的大学生，而其编写CIH病毒的目的居然只是想让一家吹嘘自家产品的杀毒软件公司出尽洋相。

T恤衫、牛仔裤，一副眼镜，瘦弱的身材和白皙的脸庞，这一形象根本让人无法与一个超级病毒的制作者联系在一起。而正是这个文质彬彬、书生模样的大学生，几行简洁的程序，几乎给整个计算机世界以致命的撼动。

陈盈豪中学时便表现出了对计算机的浓厚兴趣和很强的理解能力，因为家境较为贫寒，他时常旷课到有计算机的同学家里去鼓捣电脑。高中时便在同学之间小有名气，他的书包里没有和同学们一样的大学教材，取而代之的全是有关电脑编程的指导书，并时常露两手让那些自吹电脑技术高超的同学无地自容。在大学里他少言寡语，上课时埋头于那些砖头般的计算机书籍中，而对老师的课程讲解充耳不闻，下课铃声一响他就回到学校的机房打开电脑，对于社交、谈恋爱等时下大学生们的“必修课”几乎毫无兴趣。大学的同学们常常喜欢聚在一起比试编程水平，在同一个试题要求之下看谁能编出代码最精悍而功能最复杂的程序来，但这种比赛已很难引起陈盈豪的注意，他认为这些东西对于自己来说，就如同一个老年人面对一堆积木一般无聊，而这无疑会招来同学们对这个一向自诩计算机高手的文静书生的讥讽。为了展示自己的实力，他按照同学的要求轻松地编写了一个只有三行，却可以同样满足目的的简洁程序，使一些计算机专业的学生也自叹不如。而在最后陈盈豪因CIH被查办时，他的那些同学对此事丝毫不感觉诧异，相反他们倒是认为这件事对陈盈豪来说，“不过是小菜一碟，他完全有这个能力，没什么好惊奇的。”

与其他计算机用户一样，陈盈豪在使用电脑的过程中经常遭遇电脑病

毒，于是他省吃俭用购买了正版的杀毒软件安装在计算机中。但这些在广告中号称“完全查杀，无一漏网”的杀毒软件，实际功效却很令他失望，甚至可以说，这些昂贵的程序毫无用处，陈盈豪找到杀毒软件的经销商要求赔偿自己的损失，却被告之这根本不可能。陈盈豪觉得自己被欺骗了，对于计算机有着深切了解的他知道，别说对未知病毒，就算已知的病毒，只要病毒的制造者简单修改一下病毒程序的代码，就会躲过那些只能呆板地按照病毒特征码进行一丝不苟工作的杀毒软件，为了“保护我自己的利益，同时也让那些自命不凡的杀毒软件见识一下什么叫不可查杀的病毒，我决心做点什么，告诉那些被蒙在鼓里的人，什么人工智能、防未知病毒入侵技术，说得天花乱坠，其实全是唬人的东西”。

这个一向以程序简洁著称的编程高手在短短的时间内，用学校的计算机一共编写了五个版本的CIH病毒，前两个版本因为破坏性不够理想被他本人销毁了。从1.2版开始，他不断加入更具破坏性的代码，并在大学的计算机中有意安装病毒测试破坏效果，由此造成了数台计算机的瘫痪，并因此被学校记大过处分。而在他看来，这个大过处分恰恰证明了自己程序的有效，是对自己“成绩”的一种肯定。

为了避免严重事件的发生，在这个版本的病毒代码中，他加入了“病毒已植入，请不要再次开机，并请专业人士维修”的警告语，希望那些不幸中招的用户将损失降至最低。同时他没有主观上散布病毒的意愿，只是不断地在小范围内测试和完善自己的程序，而不知何故，病毒不经意间被连接到互联网上并传播开来，“这是我始料未及的，也是我追悔的原因之一。”

CIH是陈盈豪的名字缩写，而病毒的发作期为26日，因为26是他的高中学号。在被捕之后，陈盈豪交代说目前已经开发出第二代的CIH病毒的核心代码，这种第二代病毒不但可以破坏个人的电脑，而且还可以通过对计算机网络的主服务器进行渗透和复制，使网络服务器的主机完全瘫痪！这让当局大感震惊，而让调查人员感到意外的是，这个病毒的制作者竟然

不会“解毒”。“第二代病毒的发作机理决定了以我目前的能力，无法在病毒发作之后做修复处理，至少以我本人的能力，无法在硬盘数据不丢失的前提下做任何有效修复。”如果连陈盈豪本人都对自己编写的病毒无能为力，那么一旦第二代病毒散布出去的话，对于计算机世界将产生毁灭性的打击。再三地追问下，陈盈豪发誓说第二代病毒因为尚未最后完成，一些代码需要进一步修改，故而只保存在他的计算机里，完全没有传播出去的可能。

为保证万无一失，当局要求陈盈豪销毁他自己计算机硬盘中的所有数据，并把源代码交由相关技术人员处理，同时交代了病毒详细源代码和发作特征等重要信息。不久，破解病毒的机理得到开发，几乎所有反病毒厂商都得到了一份可以破解第二代CIH病毒的查杀代码，而对第二代病毒有着深入研究的技术人员声称，在病毒的编写思路和程序代码的简洁这两方面，不得不佩服陈盈豪的天才。

然而就是这样的一个天才，却患有严重的抑郁症。

他展示给同学们看的程序，对反病毒公司的挑战以及CIH病毒的编制动机，都是他抑郁得不到释放的具体表现。陈盈豪在接受“台湾刑事局”的调查侦讯后开始变得极其狂躁。据其所服役部队的军医介绍说，陈盈豪３月份被批准接受精神科医生诊断，并咨询了心理调剂师，而经陈盈豪母亲确认，陈氏家族有着不同程度的精神病病史。

因为身体原因，陈盈豪暂时未受到刑事处理，为了逃避今后刑事处罚，陈盈豪居然想以自己的计算机技术为筹码希望得到军方的庇护。他对军方声称可以在短期内设计出一种可以导致敌方电脑系统瘫痪的程序。起初，军方对此兴趣十足，甚至多次开会表决，准备让这个仅凭几行代码便让世界束手无策的年轻人充当信息战的专家；但在他被确诊为具有家族精神病史，自控能力有问题之后，军方则要求他立即退役，以免他在未行之有效地对敌人信息产生破坏之前，因精神问题首先破坏掉了己方的军用计算机系统。

在整个计算机发展史中，黑客与病毒制作者是两个有区别的概念和人群，他们对计算机的控制手段和相应的行为目的并不相同。黑客为了达到自己非法入侵对方系统的目的，时常会借助计算机病毒的帮助；而计算机病毒为了达到破坏系统的目的，也经常通过黑客之手以程序的形式入侵计算机，并得到最高级别的控制权。二者互为依靠，根本无法截然分开。在黑客与计算机病毒的编写者相互之间的技术借鉴和交流过程中，反病毒软件也充当着反黑客与反病毒的双重角色。在这场“魔高一尺，道高一丈”的攻防对抗中，黑客技术与病毒技术紧密结合同步演变，而反病毒技术因为目前被动的防治原理决定着它只能跟在黑客与病毒之后亦步亦趋，无法在真正意义上赶在病毒前面对未知病毒进行有效地查杀，因为反病毒厂商永远无法知道下一个病毒会以何种机理、何种技术手段出现，他们只能在病毒出现后努力在最短的时间内找到病毒的特征码，再进一步通过分析病毒程序从而研制出防治手段，而往往这种手段因为越来越先进的病毒技术、反查杀能力及病毒自身修复功能的不断强大而显得力不从心。很多中毒电脑虽然经过反病毒软件的杀毒，但其重要系统文件因为被病毒破坏无法完整修复而不得不重新格式化硬盘，致使很多重要数据在杀毒软件的严密监视下仍然难保平安，于是对于黑客和病毒的制作者很多计算机用户都是深恶痛绝，却又无可奈何。在不断完善的计算机保护法规对黑客与病毒编写者的不断大力打击之下，病毒制作者不但毫无收敛之意，甚至为了嘲笑杀毒软件的无能，而加大力度研发更先进、更灵活、更难以剿杀的病毒程序，能够让你我的计算机世界随时陷入新的危机之中。

世界医疗部门有一个只针对计算机界的新生病理名称，名为“电脑自闭症”。患这种病症的人都是一些计算机界的顶尖高手，他们个性偏激、不善于人际交往，对社会现状的不满往往表现在对计算机空间的恶意破坏上，因为只有在计算机领域中的征服感，才能让他们拥有心理上的满足。他们一般显得木讷，与现实社会格格不入，但在计算机面前，他们却激情澎湃、反应敏捷，对计算机的超强理解和操控能力。在性格缺陷的影响

下，使得他们往往处于一种狂躁的无法自制的不安和兴奋之中，而这种兴奋和不安往往不受自身约束，只有在对他人产生影响，并引起别人的关注之后才能真正平静下来。

负责侦办CIH病毒一案的李相臣认为陈盈豪是电脑界不可多得的人才，但他家庭条件一般，且患有比较严重的精神躁郁症；除了精通计算机技术外，对于社会生活的其他方面表现出超人的弱智，所以退伍后恐怕很难找到工作。为此，李相臣向陈盈豪表示，如果他退伍后找不到工作就来找他，一定会帮他介绍一份好的工作。

但愿有了李相臣的帮忙，陈盈豪可以安分守己地做自己喜爱的事，而把注意力转移到与CIH无关的事情上。若非如此，那么对于世界计算机领域来说，这可不是个好消息，那些自认“技术一流，完全查杀”的反病毒公司，除了要改一改广告词之外，还是会感觉如坐针毡。

2000年，陈盈豪被美国网虎公司聘为硬件工程师，负责新一代具备预警机制的主板等硬件的研发工作。在2001年的一次采访中，提到令世界谈之色变的CIH，陈盈豪承认造成如此严重的后果是出乎他本人意料之外的。他表示“自己日以继夜地工作，希望得到大家的信赖，忘记他曾经犯下的错误”。对于曾经热衷于编写的电脑病毒，陈盈豪说，“一辈子再也不碰了。”

【黑客知识】

主板BIOS：一台计算机最基本的构成一般可分为硬件和软件两个部分。软件部分为操作系统和应用软件；硬件部分又可简单分为主板、硬盘、内存、显卡、光驱、显示器等。BIOS（Basic Input/Output System，基本输入输出系统）全称是ROM－BIOS，是只读存储器基本输入/输出系统的简写，它是主板上的一小块集成电路，其作用是为电脑提供最低级、最直接的硬件控制程序，从而

让一台刚刚启动的计算机在未启动主操作系统之前，让计算机清楚地分辨出本台计算机的键盘、鼠标、硬盘容量、系统日期等一系列设置，将这些基本的硬件初始化，并通过自身的功能使系统能快速地找到相应的硬件驱动程序，同时将硬盘中用以启动操作系统的零磁道信息传入中央处理器，以保证计算机最基本的启动要求。

病毒特征码：计算机病毒在潜入计算机后一般不单独以文件的形式存在，而是将自身合并到系统正常的程序文件中，因为合并了程序，所以大多数病毒会使系统文件的长度有所增加，少数病毒通过改进算法，将自身合并到系统文件中但系统文件的长度并不发生变化。因为病毒也是一段程序，为了达到一定的目的，它必将要对计算机发出一系列的操作指令，这些操作指令的发布要靠一段段的程序代码来完成，而这些命令病毒执行任务的代码可以通过一系列的技术手段从病毒中分离出来，作为判断系统是否染毒的参照物，这种代表着病毒特征的代码就称为病毒特征码，杀毒软件便是通过程序自动分析计算机中的每一个文件，并自动查找这种病毒特征码来判断系统是否有病毒存在，每一个病毒的特征码都不相同，所以杀毒软件要自己从特征码库中抽取每一个病毒的特征来对应查找系统文件中的病毒，这一过程随着目前病毒数量的增加，使得杀毒软件病毒特征库也日益庞大，从而使查杀病毒的过程变得相对漫长，一般查杀一台完整的安装有操作系统和应用软件的计算机至少需要十分钟或更久的时间，有时这也取决于计算机硬盘中存储文件的多少。

附：计算机病毒界的大事简表。

1982年，Elk Cloner病毒出现。当时的计算机没有硬盘，故而这个病毒被安置在一个游戏磁盘上，在前49次使用时一切正常，当第50次使用这张磁盘进行游戏的时候病毒将阻止游戏的正常运行，取而代之的是在空荡荡的电脑屏幕上显示一首短诗。这是普遍公认的计算机史上的第一个病毒，其中玩笑的效果比其破坏性更是给人留下了深刻的印象。

1986年，Brain病毒出现，这是第一款攻击DOS操作系统的计算机病毒，该病毒会在发作时将用无效数据填满磁盘上的空白空间从而导致“磁盘已满，空间不足”而不能再继续存储数据。

1999年，莫里斯蠕虫（Melissa）病毒在几小时的时间里蔓延全球，这是最早通过电子邮件传播的病毒之一，当用户打开一封染毒电子邮件的附件后病毒自动查找当前用户保存在邮件通信簿中的前50个地址，并向其发送带毒邮件。莫里斯蠕虫的成名源于它是世界上爆发最快、影响最广的病毒之一，从第一个病毒被释放到遍布全球，只用了几个小时。

2000年，大名鼎鼎地爱虫（Love bug）病毒席卷世界。它巧妙地利用了人们对爱情的渴望，将自己伪装成一封求爱信，数小时内传遍全球，其传播速度和范围堪比莫里斯蠕虫。

2003年，冲击波病毒疯狂攻击了几乎全球各地所有使用微软操作系统的计算机并造成严重损失，这种兼有病毒侵害与黑客攻击双重功效的病毒程序利用了微软操作系统中的一个缺陷对系统的互联网端口进行大肆攻击，从而在很短的时间内耗尽系统资源并导致系统崩溃。随之而来的“震荡波”病毒工作机理与之类似。

2007年，另一个来自中国的病毒开始横行中国各地，这就是“熊猫烧香”。用户电脑中毒后会出现蓝屏、重启以及数据丢失等现象，它能中止很多知名的杀毒软件并自动搜索和删除扩展名为.gho的文件，被感染的用户系统中所有.exe可执行文件全部被改成熊猫举着三根香的模样。病毒作者李俊，25岁，武汉人，以自己出售和由他人代卖的方式，在网络上将该病毒销售给120余人，非法获利10万余元。他编写这个病毒只用了几天时间，同时让人吃惊的是，这个年轻人只有中专文化水平，而且并非计算机专业。

2009年，第一个“木马生成器”病毒产生，并在三天的时间里爬升到各大杀毒软件厂商的病毒破坏力排名榜的榜首位置。这种名为“木马下载器”的病毒一改昔日病毒需要手工编写代码的方式，由程序自动生成病毒程序，并具备超强的自身变异和反查、反杀功能，中毒的计算机会自动生成一千到两千个病毒程序，窃取重要资料和邮箱密码等数据，查杀难度相当大。

第十四章

蠕动在网络深处的虫子

我只是觉得这样做很酷，很好玩，我其实并不想因为一条看不到的虫子被人暴扁一顿。

——莫里斯

“就像人类目前无法知道银河系有多大一样，人类同样无法知道这个由人类一手制造出来的遍布全球各个角落的计算机网络有多大，在同一时间有多少电脑正在上网，有多少信息被传递。”

当讲师在讲台上讳莫如深地滔滔不绝时，美国康奈尔大学学生罗伯特·莫里斯（Robert Morris）却对讲师的这句话产生了疑问。难道人类发明了互联网，却无法侦测它的大小，对其有一个清晰准确的掌控吗？我倒要试试。

❶ “数码虫子”的繁殖地：电子邮件

电脑与互联网的飞速发展和普遍应用，使得一个真正意义上的“地球村”最终形成，人们可以坐在自己的办公桌后与千里之外的亲友进行各种方式的信息交换，可视电话与视频聊天技术的成熟使得“地球村”的各个

角落都可以实时进行面对面的交流，而在互联网上，时至今日使用最广泛的信息交换方式，应该还是电子邮件。

电子邮件的英文缩写为E-mail，是一种用电子手段提供信息交换的通信方式，是Internet作用最早、应用最广的信息处理服务之一，由于这种信息交换方式具有操作方便迅速、收费低廉、投递准确等优点而在全球范围内被广泛地使用。从1969年电子邮件技术诞生以来就一直承担着世界上40%以上的信息交换工作，几乎每一个使用电脑的人都有一个或几个电子邮箱，通过这些电子邮箱与亲友保持着信息交流。

网络上的个人用户不能直接收发电子邮件，而要通过向邮件服务商申请一个电子信箱地址作为邮件的存储和接收位置，一旦邮件服务器收到一封电子邮件，服务器就通过电子邮件地址判断接收方的位置，并将该邮件放入用户的电子信箱内，同时通知用户有新邮件到达；发送邮件与此顺序相反，用户写好一封邮件后，点击“发送”按钮后，邮件先被服务器接收，再按邮件提供的收信人地址将邮件转入相应的位置。于是，一封电子邮件的运动流程便可以理解为“发件人计算机——电子邮件服务商——互联网——收件人的邮件服务商——收件人计算机”。在这个流程中，邮件服务商的作用便相当于邮局，它将各种邮件分门别类地整理好，再送上各自该去的目的地。每天在互联网上流转的电子邮件达几亿份，这要求邮件服务商拥有强大而稳定的邮件服务器和大批量邮件的处理能力，以避免邮件收发时造成信息的拥堵。

在病毒和黑客出现在网络之后，很多思维超前的黑客与病毒制造者，开始把目光瞄到了电子邮件这种信息交换非常频繁的工具上来。通过大量发送垃圾邮件让邮件服务器不堪重负，无法迅速和有效地处理这些突如其来的垃圾信件，致使大量有用的电子邮件无法正确准时地得到处理，使网络信息的交换处于迟缓和停滞状态；而同时这些垃圾邮件的内部常常会含有一些窃取用户信息的程序代码，在收到这种含有恶意程序代码的邮件后，这些代码便进驻用户的计算机，并记录用户的操作、收集用户的各种

密码信息，再通过邮件发送到别处，从而造成用户信息的外泄。这种通过攻击电子邮件服务商来进行网络破坏和信息窃取，同时具有黑客软件与计算机病毒双重功能的程序代码，人们通常形象地称其为“蠕虫”。

计算机界有一个很有趣的现象，那就是习惯将与这些冰冷的机器有关的一些事物以生物来命名。比如人们把电脑程序编写上的错误称为“虫子”（BUG），把被黑客操控和利用的计算机称为“肉鸡”，把危害计算机正常工作的程序代码称为“病毒”，而病毒这个词原本只是用来标明引起生物体病变的。同样，人们把那些通过电子邮件系统横行于网络，从而引起信息高速公路拥挤并事故频频的恶意代码，称为“蠕虫”。

最早被命名为“蠕虫”的程序出现在互联网刚刚出现的时候。那时，维护这个无形网络的工程师们为了方便快捷地测试网络的状态，编写了一种可以畅行网络的小程序，这些程序不断地发出信息，另一些程序在别处接收他们发出的信息，通过计算二者间收发的间隔时间来判定信息网络的畅通状况。那时候，面对默默无闻、不苟言笑的电脑而觉得枯燥乏味的工程师们便自作主张，用“蠕虫”来标明这种程序，不仅生动形象，而且也算是自己无聊工作的一枚开心果。最早通过蠕虫工作原理对计算机产生破坏作用的病毒，只是一种恶作剧式的计算机动画，病毒发作时，计算机屏幕上会出现一只相貌丑陋的虫子，它四处游走，吞食着所到之处显示在屏幕上的文字，使用户无法对计算机正确的操作。

直到1998年，第一个真正利用电子邮件进行信息破坏和密码窃取的蠕虫病毒诞生了，让人吃惊的是，这个蠕虫刚一现身便震撼了计算机界，其影响力和破坏力都是史无前例的。

❷ 虫子的力量

“虫子之父”那时刚刚进入大学一年级，随即便展露出对计算机的极

高天赋，他编写的程序让他的导师也自叹不如，别的同学要几千行的程序才能完成的工作他常常只用一半数量便可以解决。当导师说到无法清晰测算同一时间世界上有多少电脑正在联入互联网时，莫里斯的好奇心便被激活了。

1988年10月以后，莫里斯一直在脑子里构思这个任务的完成方法和手段。通过一般的编程方式恐怕很难达到目的，因为在同一时间里有开机的用户、有关机的用户、有开机但没有上网的用户，而世界各地，同一时间上网的计算机用户数量是瞬息万变的，如果一定要采用编程的方法来统计，则要求这个程序一定要在互联网上极迅速地游走，并点名一样在用户的计算机里穿过并返回一个累加的数值，那么程序的运行速度也要求非常迅速。即使这样，最终取得的这个数值也只能是一个近似值。而让所有的上网者在同一时间向某一数据统计中心报告自己的工作状态来进行统计的方法显然也行不通，全球各地时间的差异、操作者的手法快慢、对这一统计的配合程度等都会让最终取得的数据准确性大打折扣，于是最理想的办法还是悄无声息地从每个上网用户的机器里穿过，不留痕迹地进行一次“暗箱操作”。

接下来的一段时间里，莫里斯开始形成自己的编程思路，并夜以继日地在计算机房里调试自己的程序。他借鉴和采取的方法就是最早测试网络运行状态的“蠕虫程序”，他设计了一段程序，让这段程序代码在整个互联网上疯狂穿行，每经过一台电脑便将数值加一。为了加快统计速度，在经过某一台电脑的同时，程序会自身复制一份并再次向别的电脑渗透，这样以几何数量级的再生能力来进行统计，应该能得到一个相对准确的数值。他瞄准了一个操作系统的缺陷作为切入点，这个缺陷来自邮件服务器寄发电子邮件的客户端程序。

1988年11月2日中午，程序已经接近尾声，连续工作了一个上午的莫里斯感觉很疲惫，他试探性地将这段尚未完全竣工的程序放入学校的局域网上，想小范围的测试一下，然后他就到餐厅吃饭去了。

在他按下回车键将程序放入到校内局域网的一瞬间，一场大祸降临了。两个小错误让这个名不见经传的大学生在短短几天内，成为全世界最知名的人物。

错误之一，学校的校内网不知被谁打开了外部网络开关，连接到了互联网上；错误之二，这段未经严格测试的程序代码算错了一个公式，使得程序在复制自身的能力上变得异乎寻常的强大。这个只有99行的程序，一旦进入互联网便会四处查找联机用户，然后破译用户口令，用E-mail系统的漏洞侵入到用户计算机中，再将自身重新复制成新的查找源，再转入网络进行查找操作。莫里斯的这个公式的计算错误不仅表现在这段蠕虫程序自身复制能力太过强大，而且在于其程序的运行原理是在已经连入互联网的计算机之间“游荡”着进行计数，虽然并没有给计算机用户带来任何损害，但一个小小的错误使得莫里斯设计的这条蠕虫不是“借取资源”，而是“耗尽所有资源”。

程序投入到互联网的那一刻起，这一小段由0和1组成的“蠕虫”，在互联网上疯狂游走并闪电般地自我复制和分裂，以超乎想象的速度在整个互联网蔓延开来。

就在莫里斯填饱自己肚子的时候，美国网络监控管理人员警觉地发现了这条蠕虫，它一经出现便摧枯拉朽般突破了用户层层防护，不请自来地进入到每台计算机里，狡猾而异常迅速地掌握了用户口令。然后利用这些口令获取了最高级别的计算机管理权，直接控制用户的电脑，得手之后立即反客为主，在网络上闪电般地自我复制，并将每一个复制品再一次投放到互联网中，分头侵入更多的计算机中。而打着饱嗝回到机房的莫里斯发现了情况不妙，再想下手阻止，却发现作为这段程序“父亲”的他居然对自己的“孩子”无能为力。

从美国的东海岸到西海岸，一台台电脑被耗尽内存资源后悄无声息地死机，各大银行、美国国家航空航天局、各大军事基地和一些知名大学的

计算机纷纷中招。众多的计算机用户和这段程序的制作者莫里斯一样，手足无措地坐在椅子上，面对着一场无形的灾难张着大嘴束手无策，莫里斯意识到自己闯下了大祸，他立即向有关部门投案自首，并第一时间将程序源代码交到相关的计算机专家手上，希望能借此减少损失并减轻自己的罪行。在10个小时之后，当那些精疲力竭的计算机专家拿出一套勉强算是行之有效的解决办法时，这条蠕虫已经横扫了整个美国，全美6000余台正在网络上工作的、基于UNIX操作系统的计算机受到感染和攻击。而在1988年，6000台基本上就是全美同时在线的电脑数量，大量的蠕虫程序充斥着网络的带宽，网络上几乎所有的机器都被迫停机。据事后统计，莫里斯这一小段程序造成的直接经济损失在9000万美元以上。

在莫里斯之前，还没有人能在如此短的时间内对整个互联网造成如此大面积的损害，而且美国法律当时也没有对这种纯技术性的信息破坏案件有明确的判例，这让那些处理莫里斯事件的法官们极为头疼。直到1990年5月初，纽约地方法庭才极有争议地判处莫里斯三年缓刑及1万美金罚款，义务为社区服务400小时，而莫里斯的律师则认为这一判决有失公允，至少没有法律依据。莫里斯事件发生之后，美国当局才针对莫里斯本人的所作所为制定了《计算机欺诈和滥用法》。

这一事件后莫里斯名声大振，几乎成为举世皆知的公众人物，美国因某个人的某件事而不得不立法，这也成为一时的笑谈。同时他对计算机技术的另类思维，表现了一个良好的计算机从业人员应有的素质，在研究生学业期满后，莫里斯成为了麻省理工学院杰出的教授。

莫里斯事件最大的影响是它给出了蠕虫程序新的定义和执行方法，同时他在程序设计中的错误，给了黑客和计算机病毒制造者提供了疯狂复制病毒自身的新算法。从此，针对互联网邮件服务器进行攻击的蠕虫程序成为黑客新宠，随之而来的这种新的攻击方式被黑客们大量采用，让反计算机侵害人士及反病毒厂商大伤脑筋。

❸ 这就是你请求的文档

1999年3月26日，黑色星期五。距离莫里斯事件已经过去11年之久，蠕虫一词正在悄然淡出人们的视线，而就在这一天，一条新的虫子突然出现在网络上。

熟悉计算机的人都知道，Microsoft Word是一个文字处理软件，与Windows系列操作系统一样出身于微软公司门下，几乎所有安装了Windows操作系统的计算机上都安装有这种文字处理工具。它功能强大且运行稳定，是排版印刷、处理公文方面的领军软件和不可或缺的办公助手。为了方便操作，在Word中采用了宏编程，用以简化常用的操作。这种宏程序简单实用，即使是非计算机专业人员也能轻松上手，编制出方便自己使用的宏代码，而正是这个入门技术要求低，且被普遍使用的宏编程方法，成就了一个名为“梅利莎”的超级蠕虫。

所有蠕虫病毒都具备两个特点：一是利用邮箱服务进行攻击；二是传播速度快得惊人。一旦这种蠕虫被放入网络，几分钟后便会游遍世界，造成巨额的损失，因为所有的应急措施在尚未激活前蠕虫已经完成了自己大部分入侵工作。梅利莎利用了几乎每台Windows都安装的Word文字处理系统和Outlook邮件收发程序，向用户保存在邮件通信簿中的前50个联系人发送邮件，当这50个人打开Word文档附件时，蠕虫再以相同的方式迅速地复制、扩散，传播速度以几何级数增长，致使大量邮件服务器不堪重负而最终导致系统崩溃。

这个包含有蠕虫的邮件标题为“这就是你请求的文档，不要给别人看”（Here is the document you asked for……don’t show anyone else），并带有一个名为list.doc的Word文档附件。当用户在不知情的状态下打开这个Word文档附件时，首先看到的是文档中包含着的大量色情网址，随即该文档中携带的宏病毒便被激活，侵入用户的计算机并开始疯

狂的自我复制。而用户电脑上保存的所有Word文档内容，都会被恶作剧般地替换为动画片《辛普森一家》的台词，使用户的机密外泄，文件内容消失。该病毒在运行之前会使Word防宏病毒警告失效，导致在宏病毒复制和扩散的整个过程中Word程序本身不作任何提示。

美国计算机紧急响应小组（USA CERT）在当天晚些时候便捕捉到“梅利莎”的踪迹，“这个周末的好心情，我早就计划好了的旅游计划全被这条虫子搅黄了，未来几天里，我们有的是活要干了。”小组成员无不抱怨，但敬业精神让他们只发了几句牢骚便立刻投入到病毒的溯源和防范工作上来。“按照病毒的发展态势，下周一开始，全球互联网将会陷入灾难，我们必须尽快阻止它。”

很快，技术人员找到了病原体的某些特征并针对病毒源代码公布了相应的处理方法，随后他们不断地完善这个方法以使病毒得以被完整的剿杀，但自身防范意识超强的“梅利莎”一次次逃脱，甚至针对反病毒人员公布的杀毒方法开发了新的变种病毒：“疯牛”。“疯牛”同样以邮件和Word附件的形式传播，但邮件的主题和附件内容全都变了，同时它将宏代码分割开来储存在Word文档的不同位置，使得剿杀难度大大增加，随后在技术人员公布针对“疯牛”的查杀方法后不久，另一个变种病毒“PaPa”又出现了，这场病毒与反病毒的攻防战越演越烈，好戏不断上演，而这场好戏，却是以千万用户的资料和密码丢失为代价的。

随着“PaPa”的出现和“反PaPa”工具的推出，新一轮变种病毒和防范工具软件你来我往打得不亦乐乎，在美国计算机紧急响应小组与“梅利莎”计算机病毒斗智斗勇的同时，FBI也开始了查找元凶的行动。让世界吃惊的是，针对一条无形的“虫子”，FBI居然出动了全部56个地方分局的警务人员，可见其重视程度。

1999年3月30日，FBI调查到“梅利莎”病毒的电子指纹与两个黄色网站有关，随后美国计算机紧急响应小组的技术分析报告指出，“梅利莎”病毒在某一个变种的宏代码中声称，对某一黄色网站提供的技术支

持“表示感谢”。FBI立即对这两个网站实施打击，强行关闭了站点服务器。在对这两个网站的调查中，FBI巧妙地找到了有关“梅利莎”病毒的序列ID，所谓“序列ID”是包含在梅利莎借以传播的Word文档的电子签名，这是病毒制作者一个小小的疏忽。通过这个电子签名，FBI找到了一个电脑黑客，而在调查中发现，这个黑客只是制作了那个以附件方式存在的Word文档，并非病毒的真正制作者。

从这个黑客的口中，调查人员证实了“梅利莎”病毒的制作者在网上有一个虚拟账号，用来追踪程序的入侵状态，通过对这个账号的进一步跟踪，技术人员最终在新泽西州找到了罪魁祸首——30岁的史密斯，一个技术相当出色的网络工程师。他仅用了三小时便制作出了“梅利莎”，而这个美丽杀手的名字，来自于计算机界龙头老大比尔·盖茨妻子的名字。

与所有的蠕虫病毒一样，这个病毒的制作者也无法针对自己编制的病毒拿出一个完美的解决方案。技术人员声称，虽然元凶落网，但“梅利莎”病毒仍然以风一样的速度在网络中肆虐，并很可能已经散布到中国、日本等亚洲国家。

“梅利莎”在极短的时间内造成了巨大的损失，包括政府、军事网络、全球定位系统的中央处理器、银行等重要部门的服务器都因被其光顾而不得不暂时关闭，同时造成了大量的信息丢失和密码错误，直接损失达惊人的12亿美元，很多人相信对史密斯的打击力度将直接起到对日后计算机病毒制作者的警告作用，一致要求严惩史密斯以达到杀一儆百的效果。在综合了各方意见之后，美国法院指控史密斯犯干扰国家公共信息通信罪、阴谋盗窃计算机服务罪，并处最高四十年的监禁及48万美元的巨额罚款。

❹ 不是核弹，胜似核弹

在明白了蠕虫病毒的攻击方式后，想编写一个蠕虫病毒并不十分困

难，只要抓住了系统的某个邮件服务漏洞，稍具计算机编程基础的人都可以“轻而易举地狠狠地搞一下，而且效果明显”。2004年出现的“震荡波”和“网络天空”病毒，其作者是当时年仅18岁的德国中学生斯文·雅尚。就是这个刚刚成年、计算机初级知识尚不健全的在校学生，却俨然成为了2004年计算机蠕虫病毒界的主角，数据显示在2004年上半年，全球恶意软件的编制技术和制作理念中，有70%要归咎于雅尚。

“震荡波”病毒在入侵之后，会以中毒计算机为服务器随机攻击网络上的其他计算机，Windows系统将会有1分钟倒计时关闭的提示。在1分钟倒数计时之后系统便会自动关闭，重新开机后这个1分钟倒计时抢先占据系统进程，从而使每次开机只能眼睁睁看着这个1分钟关机的提示信息无可奈何。

黑客技术与病毒的完美结合，使这种技术要求不高但攻击力超强的蠕虫程序成为网络上令人恐惧的东西，很多电子邮件的使用者在打开邮件时都不得不高度警惕，但仍不断有人中招。“蒙面客”蠕虫病毒的感染者其典型症状是不断地向外发送病毒邮件，更让用户焦头烂额的是这条可恶的虫子可以通过窃取击键记录，从而破解用户的密码信息导致用户隐私的泄漏。该病毒在法国、印度、新加坡和中国台湾地区传播广泛且危害巨大，它同样利用邮件进行传播，并带有一个附件。它的厉害之处在于，当邮件接收人开始有所警惕并对所有Word附件进行特别关注和用前查毒时，病毒的制作者不再使用Word文档作为附件，转而采用“漂亮女生、爱情、音乐、照片、屏保”等诱人的字眼作为附件关键字，并用一个伪造的文件格式来命名它可执行文件的本来面目，从而使用户放松警惕，落入病毒精心设计的圈套之中。

几乎所有的蠕虫病毒都算不上高科技，唯一让调查人员感到有较新编程理念和技术含量的蠕虫病毒就是大名鼎鼎的“红色代码”。

“红色代码”病毒是一种具有超前编程理念的新型网络病毒，充分体现了黑客技术与病毒相结合的威力，它将蠕虫、病毒、木马程序有机整

合，成为一只“毒性超强”的蠕虫，有些计算机业界人士甚至称其为“划时代的计算机病毒”“开创了病毒领域的新高峰”。这种病毒只要成功地取得了被入侵的计算机管理员口令，便可以为所欲为地对计算机进行各种非法操作，销毁硬盘数据、盗走机密文件，恶意修改密码、堵塞网络通道，可以说恶意程序能进行的任何破坏行为它都能做到有过之而无不及。它并不将任何有关病毒本身的信息写入被攻击服务器的硬盘，它的程序本体只是在用户的计算机内存里一闪而过，借助这个服务器的网络连接攻击其他的服务器，直接从一台电脑内存转移另一台电脑的内存，属于跳板式的攻击。因其攻击目标很少为普通的个人电脑，其注意力直接放在攻击网络服务器上，从而直接使网络服务器被毁，而这种新型的、隐蔽性极强、查杀难度极高的蠕虫病毒也是第一种在中国境内大面积入侵的蠕虫病毒，或者换句话说，这是一种专门针对中文操作系统的蠕虫病毒。

随后出现的第二版“红色代码”首先会判断机器是否已被感染，如果未被感染，则病毒立即在系统中创建多达300个病毒线程，当判断到系统默认的语言ID是中国或中国台湾时，线程数猛增到600个，创建完毕后随机生成若干个IP地址，并让每个病毒线程每100毫秒向其中一个IP地址发送一个病毒传染数据包。如此数量庞大的病毒数据包大量占据着网络带宽，可以在短时间内使网络陷入瘫痪状态。同时这个第二版的红色代码病毒本身携带有一个木马程序，这个木马程序可以实现病毒制作者对已经成功入侵的计算机实施全程遥控，并可以通过简单地更换木马程序来随时扩充病毒的功能。

蠕虫病毒开创了计算机病毒的新局面，从而使不依赖高技术手段便可以瞬间使互联网陷入大面积的瘫痪状态，如“尼姆亚”病毒和“求职信”病毒以及最新的“SQL蠕虫王”病毒，都不是什么高新技术的体现，但其巨大的破坏性却让看似铜墙铁壁、固若金汤的互联网漏洞百出，通过简单而迅速的攻击，就会使原本畅通无阻的互联网系统变成一个僵尸网络，所有连入互联网的计算机用户都随时受到威胁。许多新病毒是利用当前最新

的编程语言与编程技术实现的，同时结合着病毒与黑客的双重身份达到破坏系统和盗取重要信息的双重作用，同时隐蔽性极强，反查杀技术和自身修复功能的使用使其极易逃脱杀毒软件的追捕，并可以快速的产生新的变种，使貌似强大的杀毒软件名誉扫地、形同虚设。

由莫里斯一手开创的蠕虫攻击技术，使黑客从最根本的以游戏网络为目的的游侠状态真正变“黑”。黑客们将目标定位在窃取重要机密文件和用户密码，破坏网络连接状态，以往那种以挑战技术极限和逗人开心一笑为目的的黑客传统“骑士精神”开始沦丧，广大普通计算机用户对黑客原来的中立印象从此一去不复返，取而代之的是对病毒和黑客的深恶痛绝。

【黑客知识】

邮件炸弹：电子邮件炸弹是最古老的匿名攻击手段之一，通过设置一台电脑不断大量的向同一地址发送电子邮件，攻击者能够耗尽邮件接受者网络的带宽，造成网络阻塞。由于这种攻击方式简单易用，能够发送匿名邮件的工具又多，所以只要对方知道具体电子邮件地址就可以进行攻击，所以这是最难防范的一种攻击手段。

电子邮件炸弹可以说是目前网络攻击中最为“流行”的一种方法，而这些用来制作恶作剧的特殊程序也称为E-mail Bomber，中文为“电子邮件轰炸机”。当某人或某公司的所作所为引起了某位好事者的不满时，这位好事者就会通过这种手段来发动进攻，以泄私愤。这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至它还能影响到邮件系统所在服务器系统的安全，造成整个网络系统全部瘫痪，所以电子邮件炸弹是一种杀伤力极其强大的网络攻击武器。

僵尸网络：僵尸网络是将感染僵尸程序的计算机自动变为服务器并向网络中的其他未染毒机器散播计算机病毒，众多的计算机用户在无意识的状态下，成为如同中国古老传说中的僵尸群一样被人驱赶和指挥着的攻击他人的工具。这一新

型的攻击方式使得整个网络可以在最短的时间内陷于堵塞状态。

僵尸网络是互联网上受到黑客集中控制的一群计算机，往往被黑客用来发起大规模的网络攻击，如分布式拒绝服务攻击（DDOS）、海量垃圾邮件等，同时黑客控制的这些计算机中所保存的信息，譬如银行账户的密码与社保账号等也都可被黑客随意“取用”。因此，不论是对网络安全运行，还是用户数据安全的保护来说，僵尸网络都是极具威胁的隐患。僵尸网络的威胁也因此成为目前国际上十分关注的一个问题。然而，发现一个僵尸网络是非常困难的，因为黑客通常是远程、隐蔽地控制分散在网络上的“僵尸主机”，这些主机的用户往往并不知情。因此，僵尸网络是目前互联网上最受黑客青睐的作案工具。

对网友的计算机而言，感染“僵尸病毒”十分容易。网络上搔首弄姿的美女、各种各样有趣的小游戏，都在吸引着网友用鼠标去点击。但事实上，点击之后毫无动静，原来一切只是骗局，意在诱惑网友下载有问题的软件。一旦这种病毒软件进入到网友电脑，远端主机就可以发号施令，对电脑进行操控。

专家表示，每周平均新增数十万台任人遥控的僵尸电脑，任凭远端主机指挥，进行各种不法活动，而大多数时候，用户并不知道自己的电脑已经被控制。

附：常见的蠕虫病毒及其造成的破坏。

“爱虫”病毒：以一封“我爱你”为信件主题的电子邮件的形式传播的蠕虫病毒，2000年5月开始席卷网络，直接损失超过100亿美元。

“红色代码”病毒：2001年7月以来直接经济损失超过26亿美元。

“求职信”病毒：2001年12月开始以大量病毒邮件轮番攻击邮件服务器并堵塞其正常工作端口，使多家著名的邮件服务商被迫关闭其服务器，损失达数百亿美元。

“Sql蠕虫王”病毒：2003年1月起，主要攻击银行等重要部门的网络服务器，使银行自动提款机工作中断，网络大面积瘫痪，直接经济损失超过26亿美元。

—— 第十五章 ——
制胜网络才能掌握经济命脉

什么是推动全球战略化发展的原动力？经济。什么是阻碍经济良性发展的最大障碍？针对经济的网络犯罪。

——雅虎网络发言人的讲稿摘抄

❶ “3Q”大战

中国网民提到腾讯和奇虎360，几乎无人不知，无人不晓。在每一台中国境内的计算机上，都至少安装有这两家公司旗下的某一个产品。

腾讯公司于1998年11月在深圳成立，经过十余年发展，成为中国的网络通信之王，其主打产品QQ的注册用户甚至超过著名的MSN，奇迹般地达到惊人的11亿，成为世界排名第一的网络通信工具。中国网民打招呼也由“把你的电话号码给我”变成了“你的QQ号多少”，腾讯公司的主要产品包括即时通信、邮箱、搜索引擎、网络游戏、交友、博客等时下最火爆的网络客户端，它一出现就打乱了网络通信的鼻祖ICQ在中国的市场经营策略，逐渐成为中国互联网即时通信领域的霸主。

相比之下，奇虎360无论从规模上还是年龄上都是小弟弟。

2005年，奇虎360网络安全公司成立。开张伊始，就把全部的卖点都

押在了“免费”二字之上。

360致力于提供高品质的免费网络安全服务，拥有国内规模最大的高水平安全技术团队，旗下360安全卫士、360杀毒、360安全浏览器、360保险箱、360手机卫士等系列产品深受用户好评，使360成为无可争议的中国网络安全第一品牌。

据专业数据整理部门统计，360安全卫士是中国用户量最大的个人计算机网络安全软件，中国网民中76%安装和使用其产品，用户量超过2.86亿。360杀毒软件是中国第一个真正意义上的完全免费的杀毒软件，正式发布仅3个月用户量已突破2.2亿；360安全浏览器的网民覆盖率超过46%，用户量突破1.75亿，是微软IE浏览器之外，用户数量最大的浏览器；在以手机平台为主的移动互联网领域，360手机卫士一经发布，即受到了广大手机用户的好评并占据了中国智能手机市场55.6%的份额，排名手机安全领域第一，其下属的木马查杀、系统垃圾清理和启动加速等一系列贴心的应用程序为其赢得无数喝彩。

这本是两家井水不犯河水的公司，分别有着不同的经营方向和用户群，但却在2010年里，彼此之间毫不客气地展开了一场肉搏。战争的焦点在于，这两家公司相互指责对方的黑客行为，并声称对方提供给用户的软件中有非法扫描和刺探隐私的功能。

2010年的中国互联网界也因这一事件被炒得沸沸扬扬，成为全球网络热点。

❷ 互联网霸权

2010年5月25日，有人在网上发布消息称自己无意中发现腾讯客户端中人们习惯称之为“QQ医生”的软件会以保护QQ密码不被木马软件盗取为由扫描用户的硬盘文件，并发布大量截图。

“QQ医生”软件的工作原理与木马扫描或病毒查杀软件类似，都是通过逐个排查用户文件的方法来检验系统的安全性，这就要求软件逐一对用户的计算机文件进行扫描和检验，而如此“绝不放过一个”的方法难免会有探测隐私的嫌疑。

一周后，“QQ医生”更名为“QQ电脑管家”，本次更名实质上是宣告“QQ医生”软件已经脱离了单纯保护QQ软件安全的单一作用，转而成为一种相对独立的个人计算机安全系统软件，除了主要的系统升级外，其工作原理仍延续着“QQ医生”的核心技术，同时存在非法扫描用户信息的嫌疑。在更名之后，“QQ电脑管家”的功能有所增强，很多方面与安全软件的第一品牌360安全卫士相近。这个改变，多少让360感到如鲠在喉。

2010年7月24日，著名的《计算机世界》杂志发表文章，声称腾讯抄袭ICQ等即时通信软件的创意，并将其以“全中国计算机用户的国家公敌”之名置于业界的风口浪尖。按业内敏感人士的推测，这篇文章很可能是因360对腾讯染指网络安全软件业感到不满，而专门进行的舆论造势。由此，这两家本来没有什么交集的公司开始逐渐变得敌对起来。

2010年9月末，360公司专门针对腾讯软件发布了“软件隐私保护器”，并随时提醒用户腾讯软件正在扫描你的硬盘，窥探你的隐私。一个月后，360再推“QQ保镖”软件，第一次正面对腾讯公司发难。“QQ保镖”可以说是一款完全针对腾讯QQ的软件，“QQ保镖”可以监视QQ软件对系统的修改、扫描，并声称可以去除QQ聊天程序以外腾讯公司强行安装在用户系统中的包括QQ新闻首页、QQ秀、QQ音乐、QQ宠物等各种附属功能，并可以由用户自主选择是否安装这些腾讯软件，而在先前的腾讯QQ软件安装过程中，这些组成部分是强行合并安装的，你若想使用QQ聊天功能，就不得不安装这些附属软件。

这一举措无疑大受欢迎，毕竟很多用户只是使用腾讯软件中的网络即时通信功能。

在首轮交钱中，奇虎360重拳出击，首战告捷。

但这一举动显然触及了腾讯公司的利益，毕竟这些附属功能是腾讯用来推广产品和广告的主要渠道，奇虎360此举等于给了用户一把斩断腾讯四肢的利剑。

❸ 一个艰难的决定

时间到了2010年11月15日，瑞星公司发布报告称，公司研发人员在分析360安全卫士的软件管理功能时，发现360安装目录下存有一个内容经过360加密的怪异文件，经瑞星公司解密后确认这是一个拥有一万多条用户隐私记录的文件夹。“其中内容充分显示出奇虎360公司对于用户电脑上所安装的软件产品、公司信息、用户桌面快捷方式等隐私有非常细致的了解。”同时瑞星公司还发布了一个名为“360信息库查看工具”的软件供用户下载使用，由用户自行检测360软件在自己的电脑中所收集到的信息，随后不久，该自检软件下载链接被取消，很多用户把抢先下载的这个软件作为纪念品收藏起来，成为“3Q之争”的笑谈。

2010即将结束的时候，两大公司的口水战也达到了巅峰，奇虎360把“腾讯非法窥探”作为撒手锏，腾讯则声称奇虎360的“QQ保镖”为非法外挂软件，二者不约而同地将对方告上了法庭。

2010年11月3日晚，腾讯公司以首页广告、强行弹窗等方式通知广大腾讯用户：“当您看到这封信的时候，我们刚刚做出了一个艰难的决定，在奇虎360公司停止对QQ进行外挂侵犯和恶意诋毁之前，我们决定在装有奇虎360公司软件的用户系统上停止运行QQ软件。”几乎同时，奇虎360公司也拒绝在自己的360浏览器中运行QQ软件WEB版，以及所有需要在浏览器中运行的腾讯产品，360浏览器一旦发现用户试图打开腾讯的相关页面就会自动拒绝访问，并打开用户自带的IE浏览器。

360公司没有像腾讯公司一样，只要发现了对方的产品就拒绝运行，而是“你在我的浏览器运行腾讯的软件是可行的”，这显得较为大度。

一石击起千层浪，腾讯公司这种拿奇虎360没办法就把用户当作牺牲品来要挟用户的做法，引起巨大反响和热议。要求软件用户“二选一”的做法是不是太绝情，各大媒体纷纷把这一消息作为头版头条。更有用户置疑，腾讯不是否认自己有扫描用户系统的行为吗？那么，如果真的不扫描用户系统，腾讯的软件怎么得知在即将运行QQ的电脑上安装有奇虎360的软件？腾讯妄图以多年来培养的庞大的用户群来挤垮奇虎360，这分明是以用户利益为不顾，在自己大难之时，首先想到的是牺牲用户而不是保护用户，这样的公司，其可信度会有多少？

各大网站也迅速做出反应，并以投票的形式让用户选择：到底是保留电脑安全第一品牌360，还是为QQ开启生存之门。让腾讯大失所望的是，更多的用户声称：“不用QQ，我们还有MSN，还有雅虎通，有UC，而计算机安全的第一免费品牌360是无可替代的。”这可乐坏了MSN、UC等国内外同行，据说在QQ与360激战正酣时，这些即时通信软件的注册用户量都大幅提升。

在2010年的最后一个月里，经过各方努力，二者终于达成和解，广大网民们终于可以摆脱“池鱼之苦”。人们不禁要问，一个企业如果想做强做大，是不是应该视产品的用户为上帝呢？一切以用户的利益作为出发点，似乎才是企业生存发展的根本途径，凡事先把用户的利益放在一边，甚至以用户利益作为要挟，未免有些鼠目寸光。

虽然整个事情都处在双方的互相指责中，但很多人推断在这一事件的背后，一家名为康盛创想公司的转向他投是双方发生争端的起因。康盛创想是有着多年实际运营经验的中国最具规模的论坛系统制造商，2010年这家公司由原来的与360公司合作转而投向如日中天的腾讯公司旗下，成为腾讯的子公司。双方都与康盛创想多次接触，并希望康盛留在自己这边，也许正是康盛创想公司的“变节”引发了这场旷日持久的“3Q”之争。

【黑客知识】

垃圾邮件：这是一个适用很宽泛的电脑名词，大体上讲，凡是未经用户许可就强行发送到用户的邮箱中的包含有广告、恐怖、淫秽等不健康信息的任何电子邮件都可以称为垃圾邮件。这种邮件一般具有成批发送的特征，很多网络用户遗留在各种注册信息中的邮箱地址会被恶意收集起来，以供垃圾邮件发送者使用，一般来说，邮箱的容积是有一定限制的，短时间内接收大量的垃圾邮件，会使一些有用的信件无法正常接收，而垃圾邮件的发送者为了大面积散布信息，通常采用多台主机，甚至是有邮件群发功能的软件同时大量发送邮件，这种发送邮件的方式极易造成邮件服务器的带宽损失，严重干扰邮件服务器进行正常的邮件递送工作。

这种方式简单快捷，技术门槛较低，极易造成巨大损失，所以很多黑客在面对安装有系统防火墙等防卫措施的电脑无从下手之时，通常会转而使用垃圾邮件攻击，也能取得非常好的攻击效果，虽然目前很多邮件提供商都有反垃圾邮件的过滤器，但就如同一个新病毒在未被收入病毒特征库之前系统不会对其做出病毒判断一样，垃圾邮件发送地址是随时可以更换的，在未被邮件提供商列入垃圾邮件发送地址之前，这个地址可能已经发送了大量的垃圾邮件，顺利地完成了其使命。

目前为止，面对日益完善的计算机防护系统，垃圾邮件攻击仍是最行之有效的网络攻击方式之一。

即时通信软件：是一个终端计算机通过网络服务器与其他计算机互连并保持文字、语音、视频通信功能的软件集合体。即时通信与电子邮件、论坛、留言板等最大的区别在于它的信息交互是即时的。世界上第一个即时通信软件名为ICQ，四名以色列青年于1996年7月成立Mirabilis公司，并在当年11月份发布了最初的ICQ版本，ICQ是英文I seek you的谐音，意思是“我找你”。

目前世界通行的即时通信软件包括MSN、雅虎通、Skype、Gtalk等，国内自腾讯公司推出QQ之后，百度Hi、新浪UC，网易泡泡等也各领风骚，成为即时

通信的热门软件。

即时通信软件比电子邮件更方便快捷，比电话更省时、省力、省钱，同时兼有文件传输、视频对话等优势，已和微软Office办公系统一样，成为每台计算机必备的工具软件之一。

—— 第十六章 ——

雅虎遇“虎”：黑客面前你永远没有秘密

最锋利的武器不是刀剑，也不是核弹，而是无所不在、无往而不利的网络。网络才是我们的必杀技和战场。

——新加坡黑客“幽默的三文鱼”的MSN签名

❶ 网络拳台上的“完胜”

中国黑客起步晚，基础差，能称得上传奇的人物相对不多，根本没有能与米特尼克比肩的黑客大师，所以中国黑客的故事相对平淡得多，很多人从最初因为好奇而下载了一些黑客软件进行无目的地扫描攻击，到最后勉强编写几个拿不出手的软件招摇一番之后便销声匿迹了，几乎没有做出过什么惊天动地的事件。中国传统的儒家文化以和为贵，慎独、慎行的思想在其中起了很大的作用。或者说，中国黑客中除了凤毛麟角的几个顶尖人物之外，大多都非常平庸。

2004年9月，智利的华人区福利彩票管理机构派出专员赶赴中国新疆，专程调查一个网名“K.O”的神秘人物。

K.O是拳击专用术语，意为直接击倒对手获胜。这个神秘人物自称“K.O”显然也是非常自信的，正如他的名字，这个IP地址来自中国新疆

的黑客在短短的四个小时内侵入智利华人福彩的摇奖系统，用特定程序控制摇奖程序的运行，成功地使自己在网上购买的彩票号码中得76万智利比索。

这种流行于智利华人区的彩票系统由于规模小，投注与发行量都不是很大，因而所有程序尽可能简化，只是在公证处的监督下使用计算机程序随机挑出中奖号码，因购买者多为华人，彼此之间信任度比较高，虽然发行了近百期，但一直没有出现过大的问题。前几期头奖没有中出，奖池中的奖金滚动累加到76万智利比索时，大奖诞生。在了解中奖者信息时，人们惊奇地发现，这注彩票的购买者是通过网银交易，而交易地址居然在中国新疆。

这个只在智利华人区发行的彩票突然出现了一个来自中国新疆的彩民，而且精准到出手即中，这不能不引起怀疑。

彩票管理机构特地聘请了网络安全专家对其摇奖系统进行分析，分析的重点自然落在这个独得76万智利比索的中国彩民身上。据专家分析，这个来自中国新疆的IP地址早在摇奖开始前4个小时就对系统进行了精准的刺探，并最终将摇奖程序挂接到了一个事先已经编制好的计算机程序模块中。按这个模块的预先设定，将一个特定的数字设为中奖号码，最终使得这个中国新疆的黑客“彩民”成功的中奖。

新疆是中国黑客圈子中最为沉寂的一个省，这里几乎没有什么重大的黑客事件发生，而这个瞄准了智利华人彩票系统的黑客，无疑是个沉稳且技术高超的网络杀手。依案情分析，这个黑客很早以前就应该知道了这个摇奖系统存在着可以侵入的漏洞，并针对这些漏洞精心编制了控制摇奖的程序并成功对接到系统中，然后再按程序设定，通过网银购买了彩票，从而使得自己一夜暴富。

专家团在新疆找到了这个IP地址，它附属于一个中型网吧。通过观看案发时的录像，调查人员发现这个IP地址映射的计算机，当时被一个头戴鸭舌帽的三十岁左右的年轻男子占据着，这个男子身材偏瘦，帽子压得很

低，脸上戴着一副宽边眼镜。嫌疑人似乎对网吧的环境很熟悉，有意挑选了远离监控的角落，并侧过身子把自己的正面背对监控，加上鸭舌帽的遮挡，整个作案过程几乎没有一个正面影像被监控捕捉到。嫌疑人咬着面包，喝着矿泉水，在这台计算机上忙碌了近五个小时，然后结账离开。

虽然得到了中国新疆公安部门的大力协助，但整个案件的侦破再无进展，最终那76万比索被智利警方冻结，并未发放。

一个月之后，这家暂时停止了彩票销售的网站主页被替换，页面上镶嵌着一幅刺刀滴血的图片和一行血淋淋的字：

“本着对用户负责的态度，理论上所有的网上交易系统都应该是无懈可击的。但遗憾的是，没有完全不存在入侵漏洞的系统。这是计算机界永恒的二难推理。”

❷ 不怕贼偷，就怕贼惦记

目前国内各大银行纷纷推出网上交易系统，包括水电费、电话费、煤气费等在内的各种生活费用都可以通过网络银行进行处理，网上购物的方便快捷也使得人们的购物方式从传统的商场转移到网购，足不出户就可以得到想要的商品和服务，并由此造就了淘宝、易趣、乐淘等各大网络卖场，众多品牌店铺也由实体店转向网络店铺。据不完全统计，目前中国境内的快递公司所接受的投递业务中，60%以上来自各大网络卖场的业务单。著名的淘宝网号称“亚洲第一大网络零售商圈”，截至2010年，其注册用户已超过两亿。在享受方便快捷服务的同时，网上的买卖双方以及银行也同时针对电子商务的黑客入侵不断斗争着。

网银交易的安全性一直面临众多的挑战，针对各种各样的黑客攻击，各大银行在推出了密码卡保护之外，又以高科技手段将银行卡绑定于U盾等硬件安全保护措施之下，而各大网络卖场也将“支付宝”“手机认证付

款”等加入其中，使得网银系统更加坚固，360安全卫士等网络安全软件也纷纷开发出网购安全系统，以防止在网上交易时密码和资金的丢失，而所有这一切无疑更激发了黑客们不断挑战自身技术的斗志。据称，几乎所有中国境内的电子商务系统都遭受过黑客攻击，只是因系统防护水平极高，很少有黑客得手，也没有造成特别大的损失，但黑客针对这些电子商务网站的刺探一天不停止，电子商务就一天得不到真正的安全。

2000年1月17日下午，曾获得过“交易过程、支付配送和数据库三方面信得过网站”称号的电子商务网站“所有网”（www.soyou.com）的主页面被黑客置换。次日，“所有网”技术总监杨帆证实了这一事件，并声称其交易核心系统未被攻破，但“所有网”因黑客攻击将被迫关闭24小时。

1月17日下午4时许，登陆“所有网”的用户都惊讶地发现，“所有网”的主页面空空荡荡一无所有，“所有网”的技术人员在第一时间发现异常之后立即着手进行修复，在使用备份文件替换网站被修改的主页面后，同时也将黑客删除的几个附属文件一并恢复，此时黑客的攻击仍在继续，技术人员密切注意着系统的稳定和安全，黑客们不断修改，网站人员则不断修复，交锋约三小时后，杨帆担心系统中的用户注册数据库和交易数据丢失，被迫关闭了网站服务器。

在清理残局的过程中，杨帆发现了黑客已经上传，但还未来得及使用的一个用以替代网站主页的文件，上面留有《致“所有网”及网络用户的一封信》，信中声称此次黑客攻击是由一个在读大学生实施的。这个大学生“正处于毕业论文写作的焦虑期”，他攻陷“所有网”完全是为了缓解学业压力以及为自己的毕业论文中的理论进行实际测试，他在自己的毕业论文中声称：中国几乎所有的此类网站都存在可以加以利用的漏洞，并可以从中渔利。“所有网”使用的交易处理系统漏洞百出，根本无法保障其注册用户的信息、资金安全，此次牛刀小试，不过是让那些“所有网”用户们知道，他们所信赖的网站是多么的脆弱，而时下流行的电子商务交易

系统是多么的不安全。

黑客在这封信的最后坦白，“所有网”前些天的关于“东方快车翻译软件”销售价格被修改为“一元”的事情也是自己所为，并叫嚣“等你们打好所有的系统安全补丁，我会再来”。

网站在这里永远是处于被动的，只能迎接这些黑客的“考验”。

❸ “新浪”遭袭

春节小长假，是人们心情最愉悦放松的时候，也是黑客们最活跃兴奋的时候，原因有二：首先，中国没有专职的黑客，新年中的各大政府机构、工矿企业都处于春节的假期中，黑客们也从日常繁忙的工作中解脱出来，有了大把的空闲时间；其次，网站在春节长假期间维护人员很少，且因处于节日气氛之中而经常忽视网络异常，更容易让黑客们趁机得手。

2000年2月9日，农历大年初五，全国上下正沉浸在一片祥和的新年气氛之中，各大媒体的头版头条却突然从近日连篇累牍的大篇幅节日报道，转为“新浪被袭，网络恐慌”之类令网民们不安的报道中来。

新年的味道淡了下来，很多与计算机相关的业界人士和爱好者纷纷放下酒杯，打开电脑，在网上搜索相关信息。

中国最大的网络平台“新浪”网自2月8日下午开始遭到黑客连续长达18小时的不间断攻击，后缀为@sina.com的“新浪”免费电子邮箱系统完全瘫痪，该事件成为新世纪中国互联网界的一颗重磅炸弹，在新年的余味里让整个中国网络为之震荡，业界惊呼“狼来了”，普通网民也在各大论坛中表达了自己的担忧：“新浪”——这个号称中国技术最优、影响最大、服务最稳定、安全性最佳的第一网络品牌，若也不能在黑客的刀下保持金刚不坏之身，中国网络安全从何谈起？更有网民形象地声称自己将不得不“赤裸裸站在网络中”。

此次攻击中，黑客所采用的手段技术含量不高，但却用到了电子邮件系统的天生克星，也就是上一章中提到的垃圾邮件。黑客调动了全国各地同盟，在同一时间、不同的地点，疯狂地以垃圾邮件的形式向“新浪”的邮件服务器发动了猛攻。由于众多的黑客联合起来在同一时间，运用同样的攻击软件向固定的信箱服务器发动波次进攻，将“新浪”电子信箱系统的网络带宽全部霸占，收发送信件的网络通道完全堵塞，导致所有“新浪”注册用户在长达18个小时的时间里无法顺利完成邮件的收发工作，在“新浪”网紧急调动10余名网络安全工程师进行了长时间的对抗和修复工作之后，终于堵住了垃圾邮件的入口，击退黑客的袭击。

几天之后的2月13日，刚刚喘了口气的“新浪”技术人员又发现有大批垃圾邮件蜂拥而至，“新浪”技术人员在严援朝的带领下与黑客战斗6小时，再次宣告胜利，但不可避免的是，“新浪”也因此接到用户投诉达10余万次，有的用户直接要求索赔。

这种垃圾邮件攻击方式是典型的第三代黑客的撒手锏和出奇制胜的法宝。最初的黑客以技术性入侵为主，他们借助自己高深的计算机技术来挑战极限，而新生代黑客则绕过技术学习阶段，以短、平、快的形式快速进入黑客角色，他们没时间、没耐心去钻研相关的软、硬件技术，而是借用前辈们研发出来的黑客软件或是利用已知的攻击方式，直接瞄准某一系统就展开疯狂攻击，比如“新浪”受到的这种信息封堵轰炸式的攻击手段，就不需要很强的专门技术，每一个人都可以打开现成的软件，输入一个欲攻击地址，然后由软件合成攻击内容并完成攻击的全过程，这其间几乎不需要人为的参与，这种极简单的方法常常令花费巨资构建起来的网站在极短的时间崩溃，就相当于一个人不间断地拨打某一电话，从而造成其他人无法拨通这部电话，区别是电话因其单线通话的工作方式，只需要一台电话对其拨打就可以造成此部电话无法接通，而网站因其预留的用户通道巨大，可以同时容纳数以百万计的用户访问，所以想达到堵塞通道的目的，只有多台电脑、多种攻击软件联合工作才有可能奏效，而时至今日，对于

信息封堵轰炸这一攻击手段，技术上还没有可以完全抵御的措施。

❹ “雅虎”遇虎

巧合的是，就在“新浪”遭袭的前一天，2000年2月7日，美国东部时间上午9时许，世界知名的大型网站“雅虎”也遭受了与“新浪”同样的厄运，黑客以同样的攻击方式袭击了当时世界排名第二的网站，此次袭击的震惊程度与影响力也足以排进黑客袭击事件的前三名。

在当时仅次于“美国在线”的“雅虎”网，注册用户高达1亿，允许同时访问的数据量最大为600兆，如此宽大的数据容积让以垃圾邮件为攻击方式的人望而却步，因为小规模的攻击，“雅虎”所拥有的带宽可以很轻松的化解掉，但是“雅虎”的对手显然明白再大的带宽也有耗尽的时候。

据“雅虎”统计，事件发生时，潮水般的邮件存取请求死死堵住了雅虎的邮件服务器通道，造成邮件服务系统崩溃，高峰时系统每秒钟的数据吞吐量达到惊人的1000兆字节，这一数字相当于普通网站一年的数据进出容量，“雅虎”在美国的邮件用户中有98%无法正常使用电子邮件，同样遭殃的还有“雅虎”的新闻网和电子商务网，这三大系统同时被泛滥成灾的无效请求占据，整个雅虎只有53%的网络系统能勉强工作。

强大的攻势一直持续了近3个小时，“雅虎”的技术人员随后在铺天盖地的访问请求中搜索出大约70万个攻击IP，在邮件过滤器中封杀了这些IP之后，“雅虎”的网站开始逐渐恢复正常。唯一让“雅虎”留有一点面子的是其中央数据库安全防护体系，在此次攻击中，中央数据库安然无恙，但在遭受黑客攻击的这几小时里，“雅虎”失去了本该有的数百万次网站广告点击量，仅广告收入的损失就极为严重。

事后，网络安全界也无奈的认为：如果“雅虎”也抵挡不住这种简单

到会打字就会使用的垃圾邮件攻击，那么整个互联网就再没有可以称得上安全的地方了。

这绝不是危言耸听。

【黑客知识】

“肉鸡”：中了木马病毒或者被别的黑客入侵后留了“后门”，可以被远程操控的电脑。黑客们入侵个人电脑后一般会留下一些控制软件，并使这些软件可以在被控电脑上随系统的启动自动运行，使得该电脑只要处于开机状态就会继续被控制者操控，这些被称作“肉鸡”的电脑此时相当于控制者的一台分机，只要控制者需要，就会对这些被控电脑发送指令，而被控电脑则会无条件执行。攻击者可以在同一时间远程操纵若干只“肉鸡”同时向目标电脑发动攻击。其隐蔽性在于，被攻击方的检查一般只会扫描到“肉鸡”的IP地址，而不能检测到真正攻击者的IP，从而使攻击者被发现的可能性大大降低，成为实用型黑客非常钟爱的攻击方式之一。

微软“视窗”操作系统的两大分枝：Windows与NT

1985年11月20日，Windows 1.0正式发布，这是个人电脑用户所使用的第一个图形界面系统，随后发明的鼠标更让系统的操作变得简便起来，这都体现了新一代操作系统的方便快捷，多任务处理、可视化、图形化的特点打开了操作系统的崭新世界。随着系统的不断完善，Windows3.0、95、98，微软的“视窗”系统开始走向普及化。

1993年8月发行的Windows NT操作系统则相当于Windows的另一核心版本，这是微软公司除Windows系统外又一个里程碑式的软件。NT是“New Tech”的英文缩写，意为“新的技术”，这是一个全新的架构，比之前的Windows有很大改进，是微软公司第一个内建支持高端客户机、服务器应用的操作系统，在保证易用性和图形化的特点上，强调更高的安全性和稳定性，并提高

系统运行效率，比先前的系统更注重网络工作环境的支持和局域网服务器的安全性，成为网络服务器和局域网最理想的构建平台。

从Windows 2000开始，微软公司将这两大分支整合在一起，使产品同时兼顾NT架构的网络功能和传统Windows的易用性，如果说Windows 2000是NT的升级版本，还不如说其是取代Windows 95、98、NT以及其他商业软件平台的全新理念下的产物。随后的2001年10月，微软推出了Windows XP系统，这个系统和当初的Windows 98一样受到用户的热烈追捧，在随后的几年中，微软推出的Windows Vista、Windows7，以及在2012年推出的Windows 8都延续了微软操作系统的辉煌。

中国计算机及网络系统的致命伤：从计算机诞生的那一天起，相关的软、硬件产业便逐渐被一些IT巨头们垄断，计算机最重要的部件CPU，仍是Intel和AMD两家公司的产品占有最大的市场份额，他们引领着CPU产业的发展方向和技术趋势，其他诸如SIS（矽统）、VIA等CPU研发机构和厂商为了保证软件平台的兼容性和运行稳定性，也不得不在技术上向Intel和AMD靠拢。国内近年研发的“中国芯”，即国产CPU，由于技术和工艺等原因，主频尚不及20世纪90年代的Intel，且此款CPU主要针对于专用计算机和手机等项目开发，实用性不强，虽然目前已有使用“中国芯”的个人笔记本电脑问世，但因其主频的“瓶颈”，现阶段根本无法与Intel和AMD的产品相抗衡。在经济层面说，世界上每一台安装有这两大厂商CPU的机器都要向这两家厂商购买知识产权，无论哪一个品牌的计算机，如果号称“全自主知识产权”，类似的宣传未免都有虚假的成分在内。

除计算机硬件方面的核心CPU以外，所有软件的核心和基础则是计算机的操作系统。全球范围内真正成熟并被广泛应用的操作系统只有微软公司和苹果公司推出的计算机操作系统，苹果公司的系统大多应用于西方国家及国内的一些高端专用计算机上，仅就中国而言，个人计算机90%以上使用Windows系统。虽然世界上已经出现了不少第三方操作系统，但由于微软公司的先入为主和消费者的使用习惯等因素，第三方操作系统也大多模仿Windows的界面和操作，而且无论从

稳定性、通用性上都无法与之匹敌，国内的“红旗”软件等新兴的操作系统采用了世界上唯一免费的Linux系统内核，但系统运行不够稳定，对硬件支持不足，其系统平台上可使用的应用软件也较少，更令人担忧的是由于Linux是源于国外的系统内核，在软件运行过程中不时会弹出英文的提示，使用时较为不便。

办公软件方面，微软的Office系统引领世界潮流，通用性极强，且经多年改进，功能强大，适用性好，成为业界无可争议的优秀产品。国内的WPS从DOS时代便欲与微软抢夺市场，并一直致力于中国办公软件的自主研发，但经过十多年的发展，最终仍不得不重走模仿Office的老路，无论从操作界面、功能模块、使用习惯上都与Office看齐，甚至连回车符号都要进行模仿，“山寨”的味道很浓。

由此看来，无论软件、硬件，中国还无法与世界一流的计算机强国相抗衡，中国高新技术产业方面底子薄、发展慢，要赶超世界领先水平，还需要多年不断的努力。

没有自主知识产权的CPU和操作系统，这不仅仅是中国计算机产业链的缺失，更深层次上，这将影响到中国的国家安全。中国的银行、证券甚至国防军事等各大关系到国计民生的部门，他们使用的计算机大多是进口计算机，人们一般会认为，国外的产品虽然价格高昂但运行稳定，而这些部门都要求计算机有较强的稳定性，但实际情况是，发达国家对中国的技术进口是有严格的限制的，出口到中国的计算机，其国际安全等级最多仅达到C级标准；软件上，几乎所有的部门都购买了正版的国外产品，以为正版就是稳定安全的代名词，殊不知微软只需要在自己的Windows系统上留下一个超级用户权限，或是故意制造一个系统隐性侵入漏洞，就可以在需要的时候随时畅游中国的各大要害部门计算机，挪走银行的资金，制造错误信息，删除或改动数据库，可以做任何他们想做的事情。若是一开战端，那些掌握着核心技术的人，只需要敲几下键盘，就可以将对手的军事部署、战役安排了如指掌，甚至他们可以发布虚假的作战命令，调动军队，让导弹无法发射，让战机无法起飞，整个战争的胜负在开打之前就已决定，这样的情形，难免让人不寒而栗。

一个现实而残酷的说法是：那些卖给你正版软件的软件制造商才是最大的黑客，是你需要面对的最大威胁，因为他们掌握着软件的最底层控制权，只要他们想，可以随时把你的电脑翻个底朝天，就像你花费巨资打造了超级防盗门，而别人手里也有一把开门的钥匙。

—— 第十七章 ——

输不起的黑客战争，信息战的必杀利器

你应该相信，即使强大到天下第一，美利坚合众国的战略军备系统也同样会输给一台冰冷的电脑。

——兰德公司发言人

“双方军事配备模拟运算结束……日期更新完成……指令已下达……模拟演习倒计时，5，4，3，2，1……”随着操作员按下按钮，一场完全由计算机推算和控制进程的模拟军事演习正式打响，时间定格在2010年2月4日。

伊朗试图威胁邻国沙特阿拉伯减少石油产量，以提高原油价格，从中谋取暴利。美国在得到这个情报后，准备派遣精锐部队到中东协防沙特阿拉伯。伊朗为了打击美国，暗中发动更为隐秘的计算机信息战。美国人发觉伊朗的这一企图时为时已晚，白宫接二连三地收到各地发来的急电：加利福尼亚州和俄勒冈州的电话系统中断；陆军在华盛顿州路易斯堡的重要基地和电话系统也中断了；就在国家安全委员会刚刚结束会议不久，一列时速320公里的客运列车在马里兰州与一列载货列车发生相撞。中央情报局分析表明，罪犯很可能是伊朗特工，他们给铁路的计算机系统注入了“逻辑炸弹”并引发了灾难。在沙特东北部城市达兰附近，一家炼油厂遭受到黑客破坏，并引起爆炸和大火；在伦敦，银行已检测出用来破坏证券

交易的三种不同的病毒。受到一系列事件打击，纽约和伦敦的股市暴跌。

2月10日，美国下令派部队前往中东。但是，由于计算机化的“电子进攻”阻塞了驻军基地的军用电话系统，美国部队不能进行调遣。由于软件中的病毒严重破坏了计算机系统的正常运转，五角大楼用于协调部队调遣、装备、食品与油料配给的计划表变得杂乱无章。在华盛顿，多家银行的计算机系统出现混乱，顾客的账目被随意做了修改，金融业务被迫停止，美国有线电视网的电视信号中断了12分钟。全国性的大恐慌出现了，人们纷纷从银行提出全部存款，政府的干预显得无能为力。

2月18日，沙特两家政府电视台的新闻播音员的面孔，被替换成了敌对领导人的面孔，并且胡言乱语，号召军队发动政变推翻现政府。在五角大楼，情报部门通知国防部长，一些来路不明的计算机黑客已向美国发动了一场全面的信息战。世界各地美军基地的计算机都受到了攻击，大部分已失去了与国防部的联络。美军引以为自豪的“空中联合监视与目标攻击雷达系统”战场指挥机，也开始出现病毒感染的迹象。

2月19日，华盛顿的所有电话系统，包括移动电话全部停止了工作。由于通信的不畅，总统欲召开的国家安全紧急会议迟迟不能下达通知……

这是由著名的战略智囊团，美国兰德公司于1996年夏天倡议并实施的一场模拟战役，战役的结果让所有顶着将星的美国军界高官们惶惶不安，一些乐观派人士认为这不过是一场由计算机自编自导的蹩脚的演出，事实真的会如此吗？世界真的会输在一台计算机上吗？这是个疑问！

1 海湾战争，信息战的首次亮相

中东地区蕴藏着占世界总贮藏量1/2的石油，同时由于中东地区的阿拉伯国家自古存在的内部矛盾和美国等西方国家的政治介入使得这片土地一直处于动荡和战争之中。1990年7月，伊拉克在向科威特提出的关于石

油政策、领土纠纷、债务一系列要求遭到拒绝后，于8月2日凌晨悍然向科威特发起进攻，下午4时，攻势强劲的伊军便占领了科威特全境。

联合国随后通过反对伊拉克入侵科威特并对伊实施制裁的决议，迅速集结了由美、英等众多国家的军事力量组成的多国部队，于次年1月17日凌晨发动了代号为“沙漠风暴”的对伊军事行动，多国部队以铺天盖地的空袭拉开序幕，至地面进攻开始时，科威特战区伊军五十四万部队的伤亡率已达25%以上，重装备损失近50%，随后多国部队向伊军发起了大规模诸军兵种联合进攻，整个地面进攻历时100小时，1月28日晨宣告结束。

战后统计数字表明在战争打响之初，多国部队与伊军相比，后者以逸待劳，占尽天时地利。多国部队与之相比，人员与大口径火炮数量比为1∶2.4，坦克及重型装甲车数量比为1∶1.44，就是在这样相对优势的局面下，伊拉克方面在开战不到四天的时间里，参战的43个师就有38个被重创或歼灭，被俘6.2万人，近6000辆坦克及装甲输送车、3000门火炮和一百多架飞机被击毁或缴获，而多国部队仅伤亡400余人。

这种优势下的迅速溃败让人产生疑问：当时号称世界第四军事大国的伊拉克如此的不堪一击吗？这个萨达姆自认为世界上最富有、最坚韧、最顽强的国家，为何如此的弱不禁风？

由各国军事专家对海湾战争的战后深入分析可以得出，多国部队在第一轮的空袭中就将伊拉克的地面雷达、信息传送系统大半摧毁，很多深埋于地下几十米深的伊军指挥部也被钻地炸弹直接命中，使得伊军在首轮打击后便失去了指挥能力，根本无法组织起有效的反击，多国部队的精确打击能力让世界震惊。

那么，多国部队是如何准确地掌握了伊军的战略战术情报和各级高机密军事设施的准确位置呢？

英国《新科学报》称，在海湾战争尚未开战之时，美国情报部门便获悉伊拉克向法国购买了一种用于防空雷达指挥的新型电脑系统，并准备通过约旦运往伊拉克。于是美国在约旦首都安曼的特工立即行动，把一套带

有窃听和传送信息功能的微型芯片安装到该电脑的主板上，这种芯片上含有一套能格式化电脑硬盘及删除重要文件的程序，被称为“AFgl”，由美国马里兰州米德堡国家安全局设计。

在首轮对伊打击之前，多国部队中的电脑精英们便通过编排好的程序激活“AFgl”的信息传送程序，于是在突袭警报拉响之后，伊拉克的防空雷达才刚刚开始工作，其雷达指挥系统的电脑便全部瘫痪，使得对多国部队的飞机来袭等雷达数据根本无法反馈到防空部队的高炮上，那些失去指挥的高炮射手只能盲目地将炮弹向敌军大致的来袭方向上胡乱射击，而多国部队的空中打击就是在这种几乎没有威胁的地面火力攻击下轻松而圆满地完成了。

在防空系统变为“瞎子”后，随之而来的由一百多架电子战飞机和六十多颗军用卫星组成的监视网将伊拉克的各种重要军事目标准确地标明在多国部队的导弹预定目标上，由于伊拉克的电子信息系统受到了预先植入的黑客程序的控制和开战以来源自互联网的轮番电子攻击，整个伊军的电脑信息系统能正常工作的不足30%，在随后的突袭中甚至有多国部队的作战飞机由于没有受到地面炮火的干扰，居然下降到距地面仅有一百多米的低空，用机炮向伊军地面目标进行扫射，“一套设计完善的计算机攻击程序，至少将损失降低了一亿美元，并将战争的日期缩短了至少一个月。”多国部队的新闻发言人战后不无得意地说。

海湾战争，是自计算机发明以来，历史上首次利用黑客和黑客软件，进行的大规模军事信息窃取和破坏的实战，国外舆论界甚至将海湾战争称为“一次信息化战争的试验场，其成果是令人震惊的”。美军在海湾战争的总结报告中称“现代战争中取胜的关键因素之一，便是在防止敌军窃取我军信息的同时，能迅速而准确地搜索、获得和处理敌方军事信息的能力，并且在这一基础之上，要拥有能控制和摧毁敌方信息源的设备和人员”。在这次战争中，由于敌对双方普遍使用计算机来进行侦察指挥，于是针对于军用计算机的入侵和破坏，以及随之带来的影响也备受各国军方

的重视，各国一方面加大本国军用计算机的安全防护工作，一方面又大力搜罗计算机顶尖人员，组织最精锐的信息战部队，力求在未来可能发生的冲突中占得先机。自海湾战争以来，各国都大力加速了军用电子信息方面的入侵和反入侵工作，也都秘密地成立了信息战部队，使之作为一个新兴的兵种进入本国的战斗序列。

❷ 一个人的战役

早在互联网问世不久的20世纪90年代初，美国的一位热爱计算机技术的上尉便做过一个大胆的军事入侵试验。

1995年秋冬之交，美国国防部组织了一次别开生面的电脑作战演习，演习的一方是联入美国军事特种网络的十余艘舰艇，另一方则是一个海军上尉。

十余艘作战舰艇正在海面上乘风破浪，而那名年轻的海军上尉则平静地坐在演习大厅电脑前。电子屏上方的红灯随着一声轻响不停地闪动起来，演习开始了。上尉开始操作电脑，调制解调器上的指示灯也开始不停闪烁，随着几声清脆的敲击键盘声，上尉在没有入网许可证的前提下将电脑接入了美国军事特种网络，几分钟之后，上尉成功地接入了一艘目标军舰的计算机系统，随着键盘不断地被飞快地按下，电脑屏幕上出现了一行文字："控制成功。"上尉取得了对这艘军舰的控制之后随即获得了最高控制密码，并进入了军舰的中央导航系统，将电子罗盘的指针强行更改成错误的方向，并以此为依据让军舰的电脑系统判断错误，将军舰驶离正确航道。接下来上尉继续控制舰上的雷达和敌我识别系统并错误的发出"发现敌舰，已锁定目标"的信息，同时舰上的电脑系统指挥各种火炮对目标进行动态跟踪瞄准。上尉抬起头，冲目瞪口呆的观众们说："现在我只要敲一下回车键，这艘舰艇便会开火，而我刚才的操作是将攻击目标锁定在

离它最近的一艘友舰上。我相信在如此近的距离上，两颗鱼雷或是导弹，就可以让那家伙到海底去观光。”

一位将军掸了掸制服上的烟灰，点了点头，在旁边的指示器上按了一下，按照演习规则这艘军舰在大屏幕上消失了。

上尉如法炮制，在半个小时的时间里相继获得了所有舰艇的控制权，当所有代表舰艇的红点在大屏幕上全部消失之后，所有的参演人员全部大汗淋漓。而那些坐在舰上电脑旁边观看的人们不敢相信，造价几千万美元，使用世界上先进技术打造的军舰，居然被一个年轻的海军上尉在半个小时里用一台普通的电脑一一“击沉”。将军说出了演习大厅里的最后一句话：“网络是危险的。”

在此之后，英国《星期日电讯报》针对这场被美国军方称作“联合勇士”的军事演习做出了这样的评论：“只要能够接入互联网，敲几个按键，任何一个具有计算机操作天赋的人都可以开创战争史上一个具有潜在毁灭性的新纪元。”

此次演习之后不到一个月，美军在一份名为《下世纪初的信息战》的研究报告中提出将信息战及相应的军力配属和人员培训等作为一个全新的作战领域和科目，报告认为“现今的网络监视与入侵技术，配以复杂的信息刺探专业人员以及由全球定位系统精确制导的高精度打击武器，所有这一切都必将深刻永久地改变战争的基本形态”。随着21世纪的来临，美国军方武库中最令世界恐惧的不再仅仅是高性能的战机、坦克和舰艇，更有从那些冰冷的电脑中发出的信息流，这些信息流的攻防能力之强，足以决定未来战争的走向。

早在20世纪70年代，世界第一黑客凯文便成功地进入了美国最机密的军事网络，随后的“潘戈”等黑客也频频洞穿美国政府各种防卫严密的网络，所幸他们只是出于一时的好奇而没有把到手的情报拿出去换钱，否则其对于美国国防不知会造成怎样的后果。

随后的黑客世界同样是人心不古，网络入侵便再无游戏的成分了，很多黑客正式瞄准了这些可以换回巨额钞票的军事机密，而费尽心思地进入那些高度戒备的网上“禁区”的。1988年，前联邦德国的一位计算机爱好者就曾把美国有关“星球大战”计划、北美防空司令部有关核导弹的资料，如广告纸一样撒到那些对此兴趣盎然的国家手中；1995年，英国一个年仅16岁的男孩在美国空军罗姆实验室的计算机网络中潜伏了9个月之久，把有关检查朝鲜核设施的相关材料打印出来夹在自己的中学课本里；1998年，一个名为“下载大师”的黑客组织公开宣称他们造访了包括美国国防部信息中心在内的6个军方通信网络，并“掌握了所有相关软件的源代码，控制了从军方通信网络到卫星接收系统的所有环节”；以色列在同一年也向美国郑重道歉，并对以色列少年埃胡德特拿入侵美国航空航天局一事表示最真诚的歉意，而美方也只能轻描淡写地用一句“希望这种破坏美以关系的事件今后不要再发生”来掩盖面对网络入侵的无能为力。

美国国家审计局在一份报告中声称，“仅1995年，入侵或尝试入侵美国军方机密网络的黑客行为就达到惊人的25万次。”事实上从计算机有了网络应用的那一天起，电脑就与军事机密有着千丝万缕的联系，各国的情报部门为了对他国的军事、经济机密进行刺探，甚至不惜重金聘请技术高超的黑客，或者花大气力培养自己的电脑入侵技术人员来达到这一目的，因为这种方式的行动成本低，隐蔽性强，而且可以在成功之后全身而退，人员安全可以保证。就算一旦败露，也可以将其称为“民间行为”而加以搪塞。

❸ 图灵和他的图灵机

计算机天生就是服务于军事的，因为当初最早的计算机研制工作，目

的就是为了服务于军事。用电脑代替人脑服务于军事领域的理念，二战中期便已初步形成，那时的军事命令和报告大多通过电报传输，而电报的弱点就是如果发送时处于同一波段，任何拥有电报接收机的人都可以接收到电报，于是军事上对电报的破译对整个战局都起着关键的作用。为了防止本方电报遭到破译，德国人开发出了一种用于加密和解密文件的密码机，名为Enigma，意为“谜”，这种用金属齿轮和转子组合在一起的机器能够通过随时更换转子，来改变文件的加密方式，从而让敌方的电报破译者无从下手。英国科学家图灵针对Enigma的特点，同样发明了一种只用齿轮和转子便可以破译德军密码的机器，而且这台被称作Colossus的设备在后来情报战中也证明了自身的价值，最重要的是它带给了图灵研制先进计算机的灵感和念头。

此后，图灵发表了众多的有关“自动计算的机器”方面的论文，并成功地编制了第一套可以模仿人脑对事物进行判断并选择最佳方式行动的程序，他无法在当时的科技水平下开发出一台真正实用型的机器，但他曾经严格按自己编写的程序和算法用纸和笔模仿一台机器与人进行了一场别开生面的国际象棋比赛，他研制的“图灵机”曾经在理论上战胜过人脑，他发明的“图灵测试”至今仍是人工智能领域最经典的测试和理论基础。

即使这样，“图灵机”所代表的先进算法、运算能力，以及可以预见运算速度，已经足以引起各国军方的注意了。二战后期，美国率先开始了研制计算机的试验。1946年，世界上第一台电子计算机ENIAC在宾夕法尼亚大学研制成功，其目的是为了快速准确地计算出炮弹的飞行弹道，为火炮的远程射击提供数据参考。在此之后，随着电子技术的快速发展和互联网的应用，从作战指挥、雷达跟踪分析、作战计划拟定，直至最终战役的实施，计算机都首当其冲起着重要的作用，计算机使得数据的计算和分析更快捷、信息传递更迅速，甚至在很多时候，只需要按几下键盘便可以发起一次军事打击行动，那战争没有硝烟，但却绝对致命。

❹ 军事网络攻击的现实威胁

从战马嘶鸣、刀枪并举的冷兵器对决到火药武器数百米距离上的步兵对射，再到导弹、飞机的超视距攻击，直到现在互联网成为新的战场，随着社会文明的进步和科技的突飞猛进，战争的形态也在发生着翻天覆地的变化，人类的文明史在某种程度上可以称作一部战争史。战争也因为这种最新式的跨越时空的信息对抗而被重新赋予了新的概念。信息战也不仅仅包括直接在互联网上对敌方军事、经济的破坏和攻击，还包括在敌方武器系统的芯片中预先植入病毒程序，比如在军机、导弹、军舰等设备上所使用的芯片中事先安插入一些相应的程序代码，这些代码平时悄无声息地潜伏在那些武器系统中，如果爆发战事，这些代码扮演的很可能就是特洛伊木马的角色，它们会让敌方的飞机不能起飞、导弹失效、军舰迷航。在越来越倚重于计算机协同工作的今天，这些信息设施的瘫痪无疑会使一支强大的军队在战场上进退失据，陷入致命的被动之中。

2002年，美国间谍得知俄罗斯方面以民间采购的形式从英国购买了600台大型计算机，而这些设备的最终货主是俄罗斯军方，于是在英国的协助下，这些运算速度极高的计算机在被植入了大量的自毁程序和木马病毒后提供给了俄方，这些程序平时不发作，一旦需要，便可以通过互联网人为控制，从而将这些计算机变为一堆昂贵的电子垃圾，而俄罗斯方面显然也是预料到这种可能，计算机到货后，便将其硬件全部拆开重新组装，软件重新设计，在最大限度地保证了信息的安全后，俄罗斯才将这些高运算速度的大型计算机投入使用。

而说到底，最终决定战争胜负的还是人，各国军方都不遗余力地培训大批计算机尖端人才，很多病毒木马的制作者，一般都比较年轻，大部分是在校的学生，这些学生黑客通常会受到军方的特殊青睐，军方会为其提供最新、最全的黑客技术培训，其中的成绩优异者也会被安全部门聘为计

算机特工人员。

美国加州大学的21岁的学生罗易林在一个晚上的时间里把校园网的六台服务器搞得乱七八糟，第二天当他坐在课堂上准备上课的时候便得到了FBI的传讯。此后这个20多岁的年轻人便得到了最周全的保护和最完善的计算机知识传授，美国在1993年批准军方实施的“国防信息基础设施（DII）”计划中，罗易林凭借自己的计算机技术在25岁时即成为该计划的中坚力量。该计划的目的是通过淘汰旧有设备，开发并装备最新设备从而提高美军对信息的分析处理能力，减少和方便未来战场上作战人员的信息处理负担，这个计划真正实施后，可以使未来战场上的那些数字化士兵只需要按几个键便可以得知友军、敌军的位置、战斗进展情况及下一步的作战任务等信息，甚至在战斗的间隙里，可以“随便和身在美国的家人用视频聊聊天”。

而作为DII计划的另一组成部分，美国将依靠在地球上空同步运转的通信卫星，建成一个全球指挥和控制系统（GCCS），该系统可以使作战部队全部统一在美国国防部的直接指挥下，并赋予国防部对战局进行全方位控制的能力。甚至在每一个局部战争中，国防部的大屏幕上可以仔细地标出已方士兵在战场上的具体位置，从而可以直观、快速地调整作战部署。这些除了武器之外，同时在身上安装有微型计算机和全球定位系统的数字化士兵所使用的信息反馈作战系统代号为“大地勇士”，每一个士兵都可以通过这套系统即时得知自己与友军的间距、弹药使用情况、战场地形及敌我军力分布、己方在当前战局条件下获胜的比率及此次战斗可能结束的时点等各方面信息，甚至在激战正酣时，它会提醒你的弹药即将用尽，或者在你被包围之后，拒绝击发你佩枪里的最后一发子弹，并提示士兵“这颗子弹是留给你自己的”。

不久之前美国声称已经研制出计算机病毒枪，其原理是利用无线电信号传播并植入计算机病毒，使传统的人为网络植入病毒的方式变得更加便捷，这种病毒枪可以用人工击发的形式向来袭的飞机、坦克、导弹等武

器的计算机系统发射含有计算机病毒的无线电磁波，一旦被这种病毒枪击中，来袭武器的计算机主控系统将会被病毒摧毁，从而丧失作战能力。

伴随着新军事革命，西方国家在军事上高度依赖信息化、网络化，美军于2005年组建了专门负责网络作战的“网络战联合功能构成司令部”[①]，担负渗透、监控、摧毁敌电子信息网络系统、窃取情报及反敌方电子入侵的重要任务。这支部队的成员几乎都是美国国内顶尖的计算机天才，平均智商140以上，被戏称为“140部队”，他们掌握着世界上最先进的网络入侵和反入侵技术。海湾战争后五角大楼一直热衷于研究这种看似强大到无所不能的所谓的“网络武器”，以期对敌人发动更为快速有效的远程网络袭击；英国军情六处在2001年就组建了黑客部队，这支拥有数百名计算机精英的部队中包括众多名噪一时的民间黑客；日本防卫省则收编了一批民间的黑客青年和计算机病毒的制作者，拼凑了一支由军中计算机专家为主导的网络信息攻坚自卫队，大力研发针对网络系统进行破坏、必要时可对敌方重要网络实施“瘫痪战”的技术和软件。印度、德国等国更是紧随其后，纷纷招募计算机高手组成本国的信息战精英部队，其他发展中国家也开始着手进行信息战的人员、设备的军事列装，试图在未来的现代化战争中获取“非对称”优势。

让我们回到本章开头的那场发生在20世纪90年代初的战争中，据称在海湾战争期间，一批来自荷兰的黑客曾与伊拉克军方接触，并承诺可以通过网络攻击获取多国部队的下一步作战计划，并可以“在适当的时候摧毁多国部队的信息控制中心”，开价是160万美元，而当时显然对信息战一无所知的伊拉克对此不屑一顾，我们现在无法想象如果当时萨达姆采用了这些黑客的建议，战争的结果会是怎样。

① JFCCNWJFCCNW：英文全称为“Joint Functional Component Command – Network Warfare”。总部位于美国马里兰州，米德堡。

【黑客知识】

图灵机：又称确定型图灵机，是英国数学家阿兰·图灵于1936年提出的一种抽象计算模型，这是一种抽象的计算模型，用来精确定义可计算函数。图灵机由一个控制器，一条可以无限延伸的带子和一个在带子上左右移动的读写头组成。图灵在设计了上述模型后提出，凡可计算的函数都可用这样的机器来实现，这就是著名的图灵论题。

图灵试验：1950年，图灵发表了具有里程碑意义的论文《电脑能思考吗？》，第一次提出“机器思维”的概念。图灵逐个反驳了机器不能思维的论点，并做出了肯定的回答。图灵提出一个假想：一个人在不知情的条件下，通过一种特殊的方式，和一台机器进行问答，如果在相当长时间内，他分辨不出与他交流的对象是人还是机器，那么，这台机器就可以认为是能思维的。这就是著名的“图灵测试”（Turing Testing）。

ENIGMA：1918年德国发明家亚瑟·谢尔比乌斯（Arthur Scherbius）和理查德·里特（Richard Ritter）创办了一家新技术应用公司，曾经学习过电气应用的谢尔比乌斯，想利用现代化的电气技术，来取代手工编码加密方法，发明一种能够自动编码的机器。谢尔比乌斯给自己所发明的电气编码机械取名“恩尼格玛”（ENIGMA，意为“谜”），乍看是个放满了复杂而精致元件的盒子，并与打字机有几分相似。谢尔比乌斯巧妙地加入了一套转子机构和一个反射器，当键盘上一个键被按下时，相应的密文在显示灯上显示，然后转子的方向就自动地转动一个字母的位置，这样下一个字母又被替换成另外的字符，如此的循环往复，当26个字母经过一个理论上的循环后重新回到起始位置时，反射器便自动进行下一轮加密工作，使得一封电报的加密方式由早期简单的字符替换方式（如只是将A替换成B，将B替换成C等）变为复式替换密码，在实战应用中，操作员只需按明文方式键入字符，机器会自动将明文转换为密文，而接收方同样在输入密文的同时便可由机器自动译为明文，同时会使任何试图破译密码的工作都变得异常困难。在二战初期，由于未能掌握ENIGMA机，德军电报一度被盟军沮丧地认为是

不可破译的。美国电影《U-571》就是以敌对双方争夺这个谜一般的电报加密机为背景的。

日本“宇宙盾”军舰事件：2007年，日本海军最机密的“宙斯盾”系统失窃。“宙斯盾”系统全部由电脑控制，配有最先进的雷达和敌我识别系统，能够自动分析20个来袭目标，并判断出其中最具威胁的目标，并向其中10个以上的目标发射导弹，进行拦截。日本海上自卫队拥有5艘装备“宙斯盾”系统的军舰。据日本《读卖新闻》报道，横须贺海军基地的一名日本海上自卫队33岁的二级士官在工作时间利用电脑与处于他国的网友交换色情图片，而他本人上网的电脑上装有关于“宙斯盾”系统的绝密资料，由于他主动开放了电脑的相关权限，导致美国开发的“宙斯盾”战斗系统相关的绝密资料被黑客窃取，据该士官交代，这个要求交换黄色图片的网友在此次事件后突然消失，由此可以肯定，这个网友与之交往并要求其传送黄色图片的直接目的在于窃取军事机密。此次泄密事件的直接损失在数亿美元以上。

美国兰德公司：二战期间，美国拉拢了一批像图灵这样的优秀科学家参加军事工作，把运筹学、逻辑学和高等数学等运用于军事作战领域并收效良好。1944年11月，空军司令亨利·阿诺德上将建议国会利用这批人员成立一个“独立的、介于政府和民众之间进行情报客观分析的研究机构……以避免未来的灾难，并赢得下次大战的胜利”。根据这项建议，1945年年底，美国陆军航空队与道格拉斯飞机公司签订一项1000万美元的研发计划的合同，这就是有名的“兰德计划”。“兰德（Rand）”的名称是英文“Research and Development”两词的缩写。不久，“兰德计划”的参与者脱离道格拉斯飞机公司，正式成立独立的兰德公司，致力于以军事情报分析和预测为主，继而又扩展到国际、国内政策等各方面，逐渐发展成为一个研究政治、军事、经济、科技等社会各方面的综合性智库，被誉为当代的“大脑集中营”“超级军事学院”，兰德公司可以说是当今美国乃至世界最负盛名的决策咨询机构。

朝鲜战争前夕，兰德公司组织大批专家对朝鲜战争进行战前评估，并对“中国是否出兵朝鲜”进行预测，最终得出的结论就是：“中国将出兵朝鲜”。当

时，兰德公司欲以500万美元将研究报告转让给五角大楼，但美国军界高层对兰德公司的报告并未重视，然而战争的发展和结局却被兰德公司言中。这一事件让美国政界、军界乃至全世界都对兰德公司刮目相看，战后，五角大楼花200万收购了这份过期的报告，以作为警示。

1957 年，兰德公司在预测报告中详细地推断出苏联发射第一颗人造卫星的时间，结果与实际发射时间仅差两周，这令五角大楼震惊不已，兰德公司也从此真正确立了自己在美国的地位。此后，兰德公司又对中美建交、古巴导弹危机、美国经济大萧条和德国统一等重大事件进行了成功预测，这些预测使兰德公司的名声如日中天，成为美国政界、军界的首席智囊机构。

—— 第十八章 ——

从“实体消灭”到“实体瘫痪”：美军黑客部队扫描

在未来的战争中，电脑本身就是武器，前线无处不在，夺取作战空间控制权的不是炮弹和子弹，而是电脑网路里流动的比特和字节。

——美国军事预测专家詹姆斯·亚当斯《下一场战争》

❶ 美军黑客部队折戟东亚

2013年2月12日10时57分，中国地震台测定，北纬41.3度，东经129.0度发生里氏4.9级的地震，震源位于朝鲜人民民主共和国咸镜北道吉州郡丰溪里，震源深度0公里。

丰溪里！时间进入到2013年之后，几乎全世界的军备大国，都将目光聚焦到这片面积不大的丘陵荒原，美国的卫星和各种远程探测设备也都瞪大了眼睛盯着这块弹丸之地。2012年4月5日，朝鲜试射远程火箭；4月14日宣布退出六方会谈；4月25日，重新向核试验反应堆添加核燃料；5月25日，第二次核试验成功。

美国开始坐不住了。想不到小小的朝鲜，不仅如此强硬地进行核试

验，甚至也让美国针对朝鲜长达两年的网络战以彻底失败告终。

2011年元旦，针对朝鲜执意加入有核国家一事，美国军方按照国家安全委员会的指示，针对朝鲜在美国国内租用的网络服务器和相关内容，以及朝鲜本土的相关机密网络实施以“军事”和“核研发”为敏感词的网络监控，在位于朝鲜本土的四个有可能实施核试验基地的军事以及周围的民用网络实施全方位监控。

早在20世纪90年代末，美国空军就曾实施过针对南联盟的代号为“Ⅰ-战争”的网络攻击，这是有据可查的美国军方第一次大规模的网络战。由卜拉迪少校带领的三十余名美国军方计算机专家空投塞尔维亚，在塞方的严密布防之下顺利潜入塞方的雷达基地，将其串联雷达的计算机电缆线切开，暴力破解了相关的密码，将干扰病毒植入塞方计算机系统中，将控制雷达的数据库通过病毒修改或销毁，从而使塞方的雷达系统丧失监控能力，并在雷达的显示屏上显示错误信息，从而使美空军的飞机如入无人之境，直接影响了战争的结局。

回到朝核问题上，由于朝鲜在六方会谈中越来越强硬的态度，美国军方开始全面监听朝方的各种舆论，特别是针对朝鲜军方网络，以“核”为关键字，进行全方位的网络刺探，开发了自动搜寻关键字的木马程序“前卫一号”和“前卫二号”，通过开放网络植入朝鲜军方系统，并由密码专家斯迪克为首，将破译出来的各种有价值的信息报送五角大楼，其中，尤其以朝鲜的丰溪里为主要侦测目标。因为种种迹象表明，丰溪里为朝鲜最有可能进行核爆试验的场所。

朝鲜显然早有防备，有关核试验的计算机网络全部转入朝鲜本土的军用独立服务器，使用朝鲜本国研发的电脑操作系统，加装第三国开发的防火墙和病毒软件，所有进出网络的数据都要经由独立部门人为审核，并进行加密处理后才能放行。尽管如此，美国军方黑客还是通过各种渠道获取了近20个G的相关数据并成功解密，知悉朝鲜将于2013年早些时候进行

一场网络代号“土地公民”的特级机密试验，据分析可以肯定，这个所谓“土地公民”的实验，即为朝鲜的第三次核爆。

2013年1月7日，朝鲜将一些近程防御导弹解除了常规装药并销毁，同时以旧密码（即美国早已破译的密码体系）发放至全军，声称“土地公民”实验结束，同时将军事保密等级由橙色降为黄色。“土地公民”字样也从军事密码信息中消失。

美国人虚惊一场，以为朝鲜以强硬的核参与状态示众，其实不过是外强中干的叫嚣而已。韩国军方侦查表明，朝鲜在丰溪里曾经一级戒备的四个有可能进行核爆试验的坑道已经被水泥填死，坑道内部的电缆也全部抽出，这说明两点：要么是朝鲜已放弃了核爆试验，将试验点作废；要么已完成了全部核爆的准备工作，随时可能启爆。

韩美双方就朝鲜是否在紧锣密鼓地进行一场核试验展开了激烈的辩论。韩国方面认为朝鲜只差按下按钮就可以启动核试验；而美国则根据网络侦查的结论，认为朝鲜已在各方舆论和经济制裁的打击下丧失了核试验的能力和兴趣，最后，韩国人在美国列举的种种证据之前也只好闭口不言。

就在美国自鸣得意之时，2月12日，朝鲜成功地进行了第三次核爆，当量1万吨级（美国当年在日本广岛投放的核弹，当量为1.6万吨），此次核爆造成了4.6级地震，中国的吉林省安图县白河镇和长白山天池以北地区居民有明显震感，据这两个地区的居民声称，明显感觉地表晃动达一分钟之久。

而与伊朗相比，军事力量和高科技水平几乎不值一提的朝鲜，居然面对强大的美国，毫不示弱，最终取得了与伊朗截然相反的结果。当年的伊朗，由于美军方黑客的干扰，其整个核水平倒退了五年，而小小的朝鲜，不仅与美国斗智斗勇毫不畏惧，甚至无论在心理战还是网络战上，都不落下风，在核爆试验和电脑黑客战上，都未被打败。

❷ 数字化战场

美国在朝鲜战场上似乎手气极差，从20世纪的朝鲜战争到这一次的朝鲜核试验，美国颜面尽失威风扫地，大张旗鼓的网络战似乎毫无用武之地。

实际上，美国的网络战体系强大到足以让地球上任何国家谈之色变。

1953年，美军在“三八线”上收拾行李回国之后，五角大楼就建立了世界上最早的计算机网络并应用于军事分析和统计，那时计算机才刚刚发明数年时间，其计算能力、计算速度和处理能力还很有限，可以使用的软件也少得可怜，仅能最简单地完成文字处理和极其简单的数据统计，美国军方此时已经高瞻远瞩地意识到计算机将在未来统治世界。

1988年，美国防部建立了体系完善的海陆空三军计算机应急反应部队，开始大力发展军事网络方面的技术和人员贮备，并将网络空间打击力量与核技术、航母和第四代战机的研发放在同样重要的位置上。

2002年，当时的美国总统小布什签发国家安全第16号总统令，在这份机密级别为最高级的橙色总统令中，小布什明确了一个新的军种：网络战联合职能司令部，下辖信息战网络行动司令部和信息网络保障联合中心。前者负责具体的目标扫描、作战分析和任务制定以及作战计划的实施，而后者则主要负责开发相关的网络软件，培训相关的技术人员，同时针对假想敌对国的网络战进行数据统计和模拟作战训练。

布什政府在军事装备上侧重于F-22隐形战机和洲际导弹、核潜艇等实体军事工业，接替小布什的奥巴马政府更加侧重于挖掘信息网络中流动着的那些由0和1组成的字符中蕴藏的巨大杀机。2009年年初，新任总统奥巴马上任之初就高调实施了为期60天的全美军事及民用网络安全状况评估，6月1日，五角大楼战略司令部司令、四星上将凯文·希尔顿发布命令，美国军方将正式成立第七三九网络特种军，承担全美的军事网络防御任务，

并针对他国计算机网络与电子系统进行秘密侦察和必要的攻击，兵力为3800人。次年五月，七三九网络特种军正式服役于美军战斗序列，该司令部隶属于美军战略司令部，司令部设在美国国家安全局总部大楼内，原美国国家安全局局长基思·B·亚历山大四星上将任司令，全面统辖美国军事网络战的部署和训练及作战任务的实施，拥有对各军种下设的网络特种战分队的军事培训、人员部署及行动指挥权，负责统一计划、协调、组织和实施美军在军事网络空间及与军事相关的民用网络上的各类打击行动，确保美军及其盟国在全球网络上的出入自由与对敌优势。二战之后，因为退出战时紧急状态，美军宣布撤销所有五星上将，四星上将是美军和平时期的最高军衔，作为美军为数不多的四星上将，基思·B·亚历山大将军出任网络司令部司令从一个侧面证明了五角大楼对网络战的重视程度，并成为与太空司令部、战略司令部等并列的职能司令部之一。其核心领导层为白宫网络安全办公室，直接对国家安全委员会和总统负责，基思上将兼任办公室主任及总统网络安全顾问，被外界称为“网络沙皇”。

网络司令部的建立和其庞大的近三万人的专业技术部队列入军备，表明网络战已成为美军的一项全球性战略任务和独立作战样式，标志着美军网络战实现了统一指挥，遂行全面攻防作战，美军网络战部队从此迈入正规化阶段。

❸ 顶级黑客的乐园

美国全球战略体系中，网络战成为炙手可热的组成部分，并在全球战略中起着举足轻重的作用。网络司令部利用国家安全局布置在太空的百余颗间谍卫星以及在加拿大、新西兰和澳大利亚、日本等国设立数十个大型地面接收站，二十四小时不间断地接收和破译搜集到的数据，所有穿行于网络中的美国认为“有用”的信息都要经过美国网军技术中心的过滤，寻

找一些可能对美国所谓的“世界安全”构成威胁的字眼。

如此庞大的数据吞吐量和技术破译难度需要太多高精尖的网络战人才和最高深的计算机黑客技术。美国国防大学军事史专家丹尼尔·库克尔（Daniel Kuehl）断言，“宗教狂热”般热衷于网络战的美军不仅大量征召散布全美的著名黑客，上万名美军士兵也将被训练成新的专业军事黑客。美军网络司令部在全美各大院校专门开设相关的专业学科，并有组织和计划地培养大量计算机专业的优秀毕业生。在网络司令部的内部，也定期请专业人员对新诞生的网络入侵技术和软件进行分析讲座和技术培训，提高战事网络打击能力。美国军方将这种网络高端军事人才培养计划定名为“名士学术养成计划”，对外宣称是银行业的民间技术贮备计划。2012年5月，达科他州立大学、海军研究生院、东北大学和塔尔萨大学共四所学校获准参加这项计划。

网络总是与黑客有些瓜葛，网络战自然也不会只从各大学府招募初出茅庐的技术人才，毕竟，所有最高端的黑客技术不是写在各大学校的教科书里，而是存在于那些世界级的黑客脑子里和手指上，那些握着键盘就足以让整个世界谈之色变的黑客大佬们自然也成了美军收罗的对象。

国家安全局还试图从更大的范围招募黑客。2012年7月，“网络战教父”基思·B·亚历山大上将参加在拉斯维加斯举行的“防御形势”国际黑客大会，并发言鼓励民间黑客也参与到国家网络行动中来。

齐达纳，75岁高龄的美国民国黑客泰斗，曾经夺得两次世界黑客大赛的冠军，以他为技术顾问的小组已公开承认服务于美国军方，这个“视网络入侵为终生职业和终极艺术美感”的小组中，有大名鼎鼎的超级黑客，日本人凡崎川和开发了针对花旗银行的密码系统破解程序而成功挪用了7400万数字货币的伊亚·柯得伦。

达斯汀· 歇内尔，22岁时在入侵美国国会网时被捕入狱，国家安全局在对其入侵过程进行技术分析的时候，发现达斯汀采用了一种相当陌生但却有效的方法进行密码破译，这种新的算法将破译密码的成功率在理论上

提高了30%，随后国家安全局将其呈交基思上将。在接下来的测试中，达斯汀在六十余名黑客高手中脱颖而出，成为基思的网络办公室副主任，主管美国军方下属的雷神（Raytheon）网络安全公司，这家公司是个技术漏洞查修公司，专职负责使用各种手段进攻五角大楼的网络系统，从而找出美军网络防御的漏洞。在接受采访的时候，达斯汀微笑着声称：“在这里的工作就像玩一个刺激，而结果未知的网游，十分有趣和具有挑战性，每发现一个漏洞，都如同得到一枚勋章，让人由衷地产生满足和自豪。”

除了隶属军方的雷神公司之外，美军还掌握着原来为民用的诺斯罗普·格鲁曼公司和通用动力集团下属的飞达网控技术联合体，这两家公司拥有多达三十余项的领先发动网络攻击的技术专利。这些专利可以迅速有效地刺探他国电脑网络漏洞和软件后台接口，并有针对性的研发入侵的软件工具，从而窃取“有用的信息”，“使对方网络瘫痪”。为此，美国军方已与这两家公司签订了高达70亿美元的技术合同，内容就是接入“敌方网络系统中常用的工具软件和操作系统”的外接工具软件，而这些软件必须“使敌方病毒查杀系统和防火墙对其失去敏感性，无法及时报警并捕捉病毒”。

4 网战余思

美国军方的数据统计表明，全美每年要阻止近7.5万次的网络攻击。美军建立这样一支特种部队，完全是为了顺应信息化战争的需要，从而最大限度地保障美国国民及其盟国的国家安全。根据对美军黑客项目跟踪了13年并一直负责美军黑客人事管理的著名防务专家乔伊尔·哈丁（Joel Harding）的评估，时至2013年2月，目前美军共有7000名信息战专家，近10万名士兵涉足网络战体系，其中专业负责技术的至少不少于6.4万人。加上原有的电子战、密码破译部、军种统计局等相关人员，美军与网

战相关的部队人数应该在15万人左右，这意味着美军网战部队人数已经相当于近150个101空降师[①]。因在二战中作为先头部队参与盟军1944年6月6日的诺曼底登陆行动，以及在1944年深秋的“凸出部”战役中奋勇抗击德军反击而名声大噪，是美军的精锐快速反应部队之一。而五角大楼批复的网战经费每年高达30亿美元。

如此庞大的军费开支，其实际战斗力也可想而知，一旦爆发战争，这支掌握着世界最高端黑客技术的特种部队将担负渗透、监控、摧毁敌方网络系统的任务，他们可以轻易地在敌方网络系统上注入病毒或木马，或者按需要激活早已布置在敌方计算机系统中的相关程序，或者可以将和平时期就已探测到的敌方系统漏洞和后门挂接相应的入侵软件，从而用其貌不扬的电脑代替飞机导弹，对敌人发动更快速、更少流血、更“人道”的远程网络袭击。那时候，军人不必热血奋战，只需要冲杯咖啡，敲敲鼠标，就可以让敌方作战系统瘫痪，军事指挥体系成为瘸子、瞎子，甚至可以控制敌方电子能源通信等各个系统，让敌方的士兵电台中接收到的不是上级的作战指令而是杰克逊的摇滚乐。在一定的范围内，美军丝毫不掩饰其网战部队的存在和作战效能的强大。美军战略司令部前司令、空军少将布雷德利也直言不讳：“我们现在花在网络攻击上的时间远超过花在网络安保研究上的时间，因为非常非常高层的人对网络攻击更感兴趣。”

只是，一个小学生都明白的道理是，剑之双刃，伤人伤己。虽然在高科技迅猛发展的电子信息化时代中，美国作为超级大国，拥有着世界一流的网战体系和作战能力，但同美国的核威慑同理，同样面对着敌国的网战威胁，毕竟，其庞大的网战体系同样依靠着联系世界的电脑网络体系，贸然发动网络战最直接的结果就是引火烧身两败俱伤，要知道，黑客是世界性的，美国黑客部队的发展壮大，也迫使其他国家不得不建立归属于本国的高科技网战体系，军事黑客虽然有组织有纪律，不会像民间黑客那样

① 101空降师：美军的老牌空降部队，是著名的82空降师的姐妹师。

一哄而上漫无目的的群殴，但其对抗结果也跳不出民间黑客对抗中“杀敌一万，自损八千”的道理，也很可能导致自己的电脑体系同样遭到来自敌国的毁灭性袭击，导弹无法发射，雷达找不到信号，成为一团糟的混乱。

科技改变生活，也改变战争。战争在高科技的引领下，开始不再血流成河，甚至只是键盘点击速度的比拼就够了，但是，请记住，所有的战争，都是在挑战人类的道德底线，伴随着人性的沦丧。

网络战，也不例外。

【黑客知识】

六方会谈：2002年朝鲜宣布发展核武器，希望和美国进行双边会谈。美国拒绝这个会谈提议，认为会谈应该包含所有相关的国家。两国最后同意由朝鲜、韩国、中国、美国、俄罗斯和日本六国共同参与，举行旨在解决朝鲜核问题的一系列谈判。2013年1月24日，朝鲜国防委员会发表声明，谴责联合国安理会涉朝决议，称六方会谈及与之相关的有关朝鲜核问题的声明不再存在，以后不会再与任何方面就朝鲜半岛无核化进行任何形式的多方对话，六方会谈宣布结束。

网战武器类型及作战方式：网战简单的说无非就是计算机病毒木马及黑客入侵等常规方式，但因有军事统管，其针对性和破坏力相应更为明确和专一。它瞄准的不是银行密码，而是军事信息的收集和电子作战系统的毁坏。

病毒武器是最普遍采用的行之有效的代表性网战武器。美、俄、印、英、日等国军队都将计算机病毒正式列入作战武器名单之中，美军已经研制出2000多种病毒武器，日本某军用设计所公布的数据显示，日本军方针对朝鲜、俄罗斯和中国军事目标的病毒也不下1500种。病毒武器有极强的敌我识别能力，只针对有“敌国特征码”的计算机网络和电脑进行传播和破坏。与普通电脑病毒不同，它还拥有遥控功能，战事结束，或是被敌方截获时为了出于舆论的主动权，可以实现自毁，使自身消失于无形，从而让敌对国找不到任何证据，并由此占据外交的

主动权。其攻击性极强，一旦被激活，可以造成敌国网络瘫痪，金融混乱、通信中断等重大事故，造成极大的社会恐慌、甚至政治经济的崩溃。

除了病毒木马等进攻性武器外，相关的网战部队还要负责开发军用防火墙软件，针对敌国网战信息和动态及时调整和研制的对策性网络工具软件等网络防御武器，以及网络嗅探器、漏洞扫描软件等网络侦察工具。据最新消息，美国国防高级研究计划局正在研究用来破坏电子电路的纳米机器人，这种机器人可以附着于食品衣服等日常用品上携带入境，在军事间谍的操纵下，被释放于敌国的要害计算机硬件中，它不需要挂接，不会被现有的技术查杀，一旦接触到敌方计算机硬件，在相应的指令下就会如硫酸般腐蚀电路板，使敌方电子系统瘫痪。

有些技术已经取得阶段性成果。嗜食硅基电子芯片的细菌已在美国军事研究所取得突破性进展。这种细菌专吃电脑的CPU、硬盘等关键部件，使得系统无法启动，重要数据被毁，而且根本无法通过技术手段恢复。这是高科技时代的生化武器，可能造成的混乱很可能是世界级的。

—— 第十九章 ——

网络上的“禽流感”与种族歧视：计算机病毒的成因

没有了病毒，计算机将失去很多乐趣；有了病毒，计算机则多了许多麻烦。这是计算机界的二难推理。

——达克·埃文格（“病毒交换机”程序作者）

1 难道你不知道进来时要敲门吗？

1991年3月6日，星期三。荷兰首都阿姆斯特丹。

阿姆斯特尔河波光如缎，林诺格尔站在办公室打开的窗子前，大口地呼吸着清新潮湿的空气。这个下午，他的心情好极了。

“丹”是水坝的意思，是荷兰人筑起的水坝使700年前的一个小渔村逐步发展成为今天的国际大都市。钻石、鲜花以及梵高等艺术大师的名字让这里闻名于世。林诺格尔喜欢这里，喜欢充满了艺术和花香的生活。

落日余晖在对面的玻璃幕墙上反射出一道强烈炫目的光，恍惚了林诺格尔的眼睛。“这些蹩脚的装修工人，总能把恰到好处的艺术破坏得一干二净。”林诺格尔小声地嘀咕着，如果没有这些讨厌的玻璃幕墙，这个时候的阿姆斯特尔河畔的景色应该是最令人陶醉的，若不是从办公室的窗

子可以直接看到阿姆斯特尔河的壮美景色，当初林氏计算机软件公司选址时，他也不会花费巨额资金选择这幢老朽破败的旧房子，未能料到的是对面的公寓新近装修使用了大面积的玻璃幕墙，结果每天的这个时候，反射的阳光都让他的眼睛生疼。转回身，林诺格尔从贴身的口袋里摸出一支粗壮的哈瓦那雪茄，眼光在办公桌上搜寻着火柴的影子。

就在这时，一个斜系着领带的职员推开虚掩着的门脚步踉跄地闯进来，林诺格尔微微皱了下眉："难道你不知道进来时要敲门吗？"

年纪轻轻的职员神色多少有些慌张："先生，我想有件事我必须要亲自对你说。我想我的电脑，它有些故障。"

"如果你自己解决不了，你应该到我旁边的房间通知技术部的人而不是用这种事来打扰你的上司。"林诺格尔揉着眼睛，他现在最想做的事情是找块砖头把对面那该死的玻璃幕墙敲个粉碎。

"技术部的人在那里，但他们也束手无策。所以我想，我应该尽快地通知您。"

林诺格尔略显诧异地抬起头。"是吗？要知道那些技术部的小伙子们都是最出色的。"他在烟缸里灭了雪茄，跟着职员来到了办公大厅。

十几台电脑整齐划一地摆在办公大厅里，但此时电脑前却空无一人，所有的人，包括林诺格尔认为"最出色的"那些小伙子们全都围在其中一台电脑前小声议论着什么。林诺格尔分开众人挤进去，漆黑的电脑屏幕上只有光标无可奈何地跳动着，屏幕上清晰地显示出一行英文："Disk boot failure，Insert system disk and press enter"（找不到启动盘，请插入启动盘并按回车键）。这是明显的计算机主引导记录遭到破坏的迹象。

"我一向认为你们是最出色的计算机人才，这点小事也需如此的兴师动众吗？"林诺格尔摇摇头，感觉有些失望。电脑通电后的正常工作程序是从硬盘或软盘上读取系统必需的启动文件，然后由这些启动文件引导系统进入正常工作状态，一旦启动文件遭到破坏，系统将无法启动，并会出现如上的"提示"。每位员工的电脑都配有硬盘和软驱，这样当硬盘因突

然断电或计算机出错无法正常启动时，便可以转而由软驱启动，再进一步修复硬盘故障。而解决这种故障应该也不是什么高难度的工作。

“软盘启动也无效，软盘启动后用DOS命令将启动文件传给硬盘后，再重新启动，还是不行。”技术部的工作人员已经显得有些慌乱和烦躁了，要知道，公司的电脑里保存的都是相当重要的数据，一旦丢失损失是相当大的。

“从我第一次接触电脑到现在，无法启动的故障就像那些每晚伴随着我的噩梦一样，家常便饭一般，所以不必担心！”林诺格尔说着就把软驱里的磁盘拿到另外一台机器上重新制作了一张启动盘，再回来尝试着用软盘启动，还是不行，一种奇怪的念头开始占据了他的心。

就在大家被这种顽固的无法启动现象搅得焦头烂额之际，刚刚做过启动软盘的那台电脑也无法启动了，屏幕上显示着同样的信息。

“我只是在这台电脑上做了一张启动盘，它就瘫痪了吗？这故障，简直可以用神奇来形容。”经过林诺格尔和技术部人员的仔细辨认后，大家一致认为是某个恶魔诅咒般的电脑病毒光临了这家小小的电脑公司，林诺格尔视线模糊、头疼欲裂，脑海里全是那面刺眼的玻璃幕墙的反光，他揉着额头，扭身对手下人低声说：“丹尼拉电子技术前沿论坛的电话号码是多少？”

❷ 我想叫它米氏病毒

丹尼拉电子技术前沿论坛是一家私人公司，也是20世纪90年代荷兰公认的规模最大、技术力量最雄厚、手段最高超的计算机专业公司，主要致力于计算机人工智能方面的研究，创办人丹尼拉是位金发美人，也是林诺格尔在大学里的同学，“我似乎暗恋过她，但她太出色，无论是从技术的角度，还是从审美的角度，她总是随时随地能让其他人感觉到自惭形

秒。”林诺格尔这样回忆和丹尼拉的那段难忘的同窗时光。

第一台发生故障的电脑上前几天为客户制作了一个半成品的程序，昨天客户用软盘将这个程序拿回去试运行，并把改进意见存在软盘上，今天早上将软盘拿回公司，公司的电脑刚插入这张软盘准备查看客户改进意见的时候，硬盘就开始疯狂旋转，电脑关机后重新启动。

“只是用一台运行正常的电脑制作了一张启动盘，这台电脑就一样无法运行了？”见多识广的丹尼拉同样无法相信这种怪异的事情。

在经过几个小时的仔细检查之后，丹尼拉发现这两台故障电脑的硬盘被重新格式化过，而那张软盘上同样是一无所有，根本没有制作过启动盘的迹象，以林诺格尔的技术能力，制作一张启动盘应该没有问题，而只是将软盘插到软驱里敲入了两个命令便使一台正常运行的电脑彻底被毁，这只能说明，那张客户送回来的软盘上一定有一种程序，能自动将计算机的所有数据清除，并以最快的速度格式化硬盘，让所有的重要文件在瞬间灰飞烟灭。

丹尼拉小心翼翼地将那张从客户手中刚刚取回来的软盘放入计算机，在仔细的检查和分析之后，她发现软盘中存在一个异常的程序，只要软盘一插入到计算机的软驱里并对该软盘有浏览等操作时，这个异常程序便被自动执行，从而不经任何允许将计算机的存储设备中的数据全部清除，从而造成数据丢失、计算机无法启动等现象，同时这个程序具有自动复制的能力，如果软盘插入到一台未被感染的电脑上，那么这台电脑也会立即被植入这个程序，陷入瘫痪。

丹尼拉立即感觉到一股冷汗从脊背上流下来，“林诺格尔先生，你记得一个叫儒迪吉·戴尔斯坦的博士曾经发表过一篇名为《计算机病毒，一种潜在的威胁》的论文吗？”

“有印象，大概是1986年3月，在巴黎。”

“没错。你的记忆力从上学开始就一直这么好。”丹尼拉默默地坐下来。“戴尔斯坦博士在那篇论文里提到过一种被称为‘计算机病毒’的恶意程序。在这之后的1987年10月，美国得拉华大学受到一种计算机恶意程

序的攻击，后来被命名为‘巴基斯坦病毒’，这种病毒程序验证了戴尔斯坦博士的假说，具备有传染性、复制性和高危害性，而且这种病毒当初席卷了整个美国，甚至流窜到了东亚某些地方。据称这是人类第一次在实验室和论文以外见到的被称作‘计算机病毒’的程序。”

“我听说过，还有‘大麻病毒’‘黑色星期五病毒’，但这些恶意程序都只是在小范围内以实验体的形式存在着，难道我们今天真的遇上了其中之一？”

“我想恐怕是这样的，我建议您过一会儿去买张彩票试试运气。”丹尼拉不无担心地说，转回身面向镜子整理了一下自己零乱的头发，她发现自己的脸色很不好看，作为一个计算机界的领军人物，她真的希望这种刚刚发明了半个世纪的电脑系统能为人类带来一场工作方式的变革而不是一场灾难，而这个病毒的发现，说明计算机病毒已经离开了实验室步入民间，一旦这些恶意程序大面积散布开来，计算机界的浩劫便要开始了，而那些以计算机为工作的人们必将深受其害，他们辛辛苦苦几年，十几年的工作，都有可能在一瞬间化作乌有。

丹尼拉揉着手掌，每当心情烦躁的时候她就不由自主地有这个小动作。“今天3月6日，是米开朗基罗的生日。如果最终我们确定这就是一个计算机病毒的话，我想叫它‘米氏病毒’。”

❸ 计算机的末日

在随后的半年时间里丹尼拉都在埋头研究那张怪异的软盘，她同时召集了众多荷兰的计算机界知名人士共同参与研究，并最终确信这是一种攻击力很强的计算机病毒，并且病毒的发作日期是每年的3月6日。丹尼拉开始大范围的呼吁计算机使用者在1992年的3月6日注意一种被命名为“米氏病毒”的恶意程序的袭击。但那些粗心的从未遭受到计算机病毒攻击的人

们对此显然很不以为然，直到1992年的3月初。

当人们把日历翻到3月6日，一场电脑世界的大灾难真的如期而至，一场病毒风暴席卷全球。先是美国加利福尼亚的近千台电脑遭劫，接下来南非约二百家公司的一千余台电脑全部被摧毁，德国银行的数百台电脑中的用户资料全部丢失，在接下来的两天时间里，包括亚洲的马来西亚、日本、中国台湾等地的计算机系统相继受到“米氏病毒”袭击，整个世界被一小段程序搅得人心惶惶。

在互联网尚未普及的年代，病毒的传播途径只有通过光盘或软盘，而这个以大艺术家的名字命名的计算机病毒居然在短短的时间里漂洋过海，在世界范围内传播，并造成了占全球计算机拥有量几乎30%的电脑数据损坏，这简直就是一个奇迹。

这是计算机发展史上第一个电脑病毒的大面积爆发，“米氏病毒”由此奠定了其在计算机病毒界龙头老大的地位，随着“米氏病毒”肆虐，各种新兴的计算机病毒也大量涌现，而这种被形象地称作“病毒”的恶意程序，其最大的特征就是超强的传染性，一旦潜入电脑，便会疯狂复制自身，并在用户毫无察觉的状态下由一台机器进入另一台机器，由一个国家转移到另一个国家。传染性是计算机病毒在它尚未真正现身之前就被相关理论预测的最主要的特性之一。

20世纪70年代，美国人雷恩在其《P-1的青春》一书中虚构了一种能够自我复制，利用通信设备进行传播并进行破坏活动的计算机程序，并首次用“病毒”为其冠名。1983 年 11月，在一次国际计算机安全学术会议上，美国电子信息专业博士弗瑞德·科亨第一次明确提出计算机病毒的概念，并被特许将他开发的一小段病毒演示代码植入到几台个人计算机中，而在这次短暂的演示中，科亨的程序平均每30分钟便可以造成一次系统瘫痪。最短的一次，仅用时5分钟。但所有这一切都只是计算机科学家们凭空设想出来的东西，并且只是在实验状态下进行一种“看上去很有意思的科学游戏”，几乎所有的人都没有对这种能自动复制并相互传染，具有

纯生物特征的计算机程序加以足够的重视，“这只是一种想当然的成人游戏，如果我能力可及，我也可以编上两个小程序玩上一玩，但我认为这些计算机使用人员，应该不会自讨苦吃研究出这种破坏性的程序来。”

然而潘多拉的魔盒一旦开启，这些掉以轻心的计算机用户们便在劫难逃了。

1986年，一对以出售自己编制的电脑软件为生的巴基斯坦兄弟亲手将“大脑病毒”（C-Brain）投放到实验室以外。当时计算机软件业还不景气，盗版现象猖獗，而且由于法律的不健全，那些辛辛苦苦研制出来的软件被大量的仿制和出售。为了防止自己开发的软件被非法拷贝，这两个天才的计算机从业人员精心编写了“大脑病毒”（即“巴基斯坦”病毒），并将其捆绑到他们开发出来的电脑程序中一同出售。当时没有互联网，刚刚研制出来的光盘存储器——“光驱”，也因为价格昂贵很少有人问津，所有的软件载体都是软盘，这种病毒只在非法复制软件时才发作，将盗拷者的硬盘剩余空间吃掉，从而使计算机出现磁盘空间不足，无法正常运行等一系列的故障。

“巴基斯坦”病毒是有史以来第一个在计算机界爆发的病毒，从这个病毒开始，为实现各种目的而开发的病毒程序充斥着计算机界，使众多花费了大量人力、物力、财力的计算机数据如泡沫一般消失不见，人们谈毒色变，甚至用“计算机界的艾滋病”来形容这种无孔不入、防不胜防的恶意程序。有关“巴基斯坦”病毒，很多人记住了两个名字：巴斯特（Basit）和阿姆贾德（Amjad）。

“巴基斯坦”病毒的破坏性不强，而且它不消除用户的数据文件，仅以一种“系统错误”作为警告来提醒用户正在进行非法的软件拷贝，但这种程序的编写意图、实现的方法及病毒体的特征却为很多人提供了指导，很多别有用心的人开始以“巴基斯坦”病毒为蓝本制作出一些功能更强劲、破坏力更大的新型病毒，甚至出现不少病毒制作团队，专门针对某些重要部门或程序进行有目的的破坏和骚扰活动。与此同时，各类防毒与杀

毒软件公司也纷纷出场，并以“第一时间最干净、彻底的清除病毒”为广告语，投入大量资金和人力展开反病毒作战，一时间，各种病毒攻击与反病毒查杀之间的较量便不断上演。

1989年9月，“耶路撒冷”病毒使超过10万台电脑陷入瘫痪状态；同年11月，台湾爆发了“大马亲王”病毒，致使大部分银行无法正常工作；1989年10月，瑞士邮电系统部分电脑由于病毒侵入而瘫痪；第二年年初，美国的电脑病毒使得全美有17万名职工推迟一个月才领到工资。

早期的病毒传播途径有限，传播速度缓慢，随着互联网的普及和发展，新兴的以网络传播并扩散的病毒以迅猛的速度让众多的反病毒厂商惊慌失措，以前的病毒以软盘或光盘作为介质，被人为地带到世界各地。在互联网上，一种病毒的出现到漫步全球则只需几分钟或几小时，著名的“莫里斯蠕虫病毒”就在数小时之内让世界范围内的数以万计的计算机陷入瘫痪，其后的“震荡波”等病毒也风卷残云一般数日之内便给世界造成了无法估量的损失，而这些借助互联网进行大面积高速度传播的病毒，其编写技术、发作模式隐蔽性和再生性与早期病毒也有着天壤之别，早期病毒以暴力进攻损毁数据为主要方式，很少注意到隐蔽自身，查杀相对比较容易，而现在的新型病毒则选择一种更为安静和“绅士”的方式，它们悄无声息地潜入并迅速控制电脑，或者窃取用户身份、信用卡信息以及其他商业数据，或者仅仅以搞笑的心态来展示制作者精湛的计算机技术，同时组成“僵尸网络”。以整合间谍软件、钓鱼软件、木马程序等手段为一体的新一代病毒已经成为当前金融犯罪的重要工具，贯穿于整个现代经济的体系之中，成为现代经济犯罪最主要的手段和方式之一。

4 计算机病毒的起源

很多人知道，能编写计算机病毒的都是一些计算机技术方面的专业人

士，在一般性的理解上，这些人对计算机有着天然的好感和热情，像对待恋人一样对计算机情有独钟，对计算机技术有着最彻底的热爱和刻苦钻研的精神。那么这样一群优秀的计算机人士又为什么会故意用这些对自己及他人有百害而无一利的病毒程序来兴风作浪，扰乱电脑和网络的秩序呢？说来话长。

计算机病毒的起源有以下几种说法：

1、程序员报复说。在计算机刚刚普及的时候，一些黑人程序员因为种族歧视，通常无法保证工作的长久和稳定，并且工作强度大、报酬低，同伴们经常会被无缘无故地辞退，这让他们一直处于高度的疲惫和毫无安全感的紧张情绪中，自然而然的，他们会利用自己的工作之便和已掌握的高级编程技术来为自己伸张正义。很多早期的病毒，平时潜伏在计算机中并不进行任何破坏活动，一旦判断出程序员被公司辞退病毒便会爆发，曾经有黑人程序员在给银行编写的程序中每天自动检测工资名单中是否存在自己的名字，如果自己的名字在工资名单中被清除，那么病毒便被激活，从而删除银行主数据库中的重要数据。

2、游戏说。一些忙里偷闲的程序员会互相挑战，他们各自编写一段可以自我修复而又能同时删除对方程序的代码，将其放到计算机内，“看它们自相残杀，并打赌哪一段程序能坚持到最后。”这些纯粹出于玩笑而产生的游戏程序会随时判断自身是不是被其他程序破坏，如果发现自身受损便会自动进行修复，使自己始终保持着金刚不坏之躯。而这种能自我修复，同时具有攻击性的病毒，其特征与现代病毒如出一辙，那些原本出于游戏目的的程序代码为病毒编制者提供了编程思路。

这种程序间“弱肉强食”的厮杀与达尔文的适者生存理论极其相似，久而久之便被称为“达尔文游戏”，或被称为“磁芯大战”，是世界公认的计算机病毒理论之一。

3、无意识的编程错误。程序都是由人编写的，在程序的编写过程中，一些不容易被发现的错误通常会演变成对计算机的正常工作产生影响

的因素，比如著名的“莫里斯蠕虫病毒”就是这种程序的编制者本来无心编写如此具有破坏性的病毒程序，只不过“一时兴起编一个无伤大雅的小玩意”，但因为在编制程序的过程中的一些疏漏，造成了这种蠕虫病毒大量涌入互联网，同时以几何级数复制蔓延开来，造成严重的危害。

4、恶作剧说。一些计算机编程人员在程序中有意加入一些玩笑，或者是一小段与程序本身无关的游戏，再或是加上一段提示语和程序员的照片之类的东西。这些东西被触发后，不会对计算机做出进一步的破坏，只是以取乐和搞笑来向世人展示自己的存在。

5、版权保护和程序改进的需要。这个无需多言，谁都不希望自己的智力成果无报酬地被他人使用和传播，于是针对盗用自己程序之人给以小小反击和惩罚是可以理解的，上文提到的研制大脑病毒（C—Brain）的那对巴基斯坦兄弟便是其中之一。

6、反病毒厂商自己研制病毒，然后用自家杀毒软件查杀，用以宣传自己的杀毒软件产品。此类病毒的来源一直没有官方证实，但各种渠道流出的消息多少可以证明类似病毒的存在。计算机病毒的猖獗让很多用户大伤脑筋，许多人都购买正版的防病毒软件来维护计算机安全，由于杀毒软件的工作原理就是提取病毒特征码来进行判断，只有当一种新病毒的特征码被杀毒软件收入到特征库之后才有可能被杀毒软件捕捉得到，于是那些最新出炉的病毒程序常常让杀毒软件制造者无可奈何，加上杀毒软件公司林立，每家公司都想打垮其他公司，于是都想尽一切办法提升自己产品的声望，都声称自己软件的技术最先进、查杀效果最好。

怎么才能达到这一目的呢？杀毒软件的唯一作用就是查杀计算机病毒，于是“第一时间捕捉到某种病毒并可以完全清除它”便是每个杀软公司最想做到的事了。

在这种想法的驱使下，很多杀软公司甚至自己研制新病毒，并投放到网络上去，由于病毒是自己编写的，自然对于发作原理、时间、特点和危害等了如指掌。当公众意识到一种新病毒的出现时，这些杀软公司立即

声称可以第一时间查杀这种新病毒，于是自己公司的产品销量便会提高一些，久而久之这种总是能第一时间查杀病毒的软件自然成为业界最受欢迎的杀毒软件。

经常听到朋友抱怨：怎么有那么多没事做的人，整天做病毒呢？很简单，都是为了一个“利”字，利益永远是类似事件的背后推手。“熊猫烧香”病毒的作者就曾将病毒的源代码在网上公开贩卖，并在短短的时间内收入数十万元人民币。目前技术上日新月异，手段上灵活多样的计算机病毒、木马、蠕虫等恶意程序从制作到贩卖的一系列环节，在一次次键盘敲击下诞生的仅仅由若干个字母组成的计算机病毒程序的后面，是被利益驱动的人性之恶。

【黑客知识】

查杀病毒的难度在哪里？

（1）强大的复制能力：病毒的特征之一就是超强的自身复制能力，一旦病毒进入自我“繁殖”阶段，其自身的复制能力和遭到破坏之后的自我修复能力便成为让所有杀毒软件头疼的问题，采用了多线程技术的病毒在发现自身被杀毒软件破坏之后，另一线程就会立即启动进行自我修复，很难被彻底清除。

（2）极为有效的“隐身术”：为了最大限度的躲避杀毒软件的查杀，目前更多的病毒采用复杂的自我加密技术，同一种病毒，可以自动生成“面目全非”的多种版本，以不同的形态招摇过市，检测和清除这种病毒非常困难。

（3）电脑病毒的“抗药性”在增强：病毒在开发的时候就已经预见到了有朝一日自己会被杀毒软件捕获到核心代码，于是很多病毒自身就有着抵抗杀毒软件的能力，甚至一些病毒专门破坏杀病毒软件，修改杀毒软件的核心代码，使其杀毒功能改变。

“木马”的定义：《荷马史诗》中记载，古希腊人围攻特洛伊城十年未能成

功，希腊联军的将领之一奥德修斯心生一计，他将士兵藏在一些由木头制作的战马雕塑中放到战场上，当特洛伊人将其作为战利品拖入城内后，木马里躲藏的士兵乘着夜色悄悄地爬出来干掉了城楼上把守的士兵，将特洛伊城门打开，由此终于攻下了特洛伊城。后人常用“特洛伊木马”来比喻在敌方营垒里埋下伏兵，从而达成自身目的的战术。

计算机木马程序的工作特点与之相似，故被冠名为“特洛伊木马”。当一台计算机通过各种不同渠道感染了木马程序后，木马程序会窃取用户信息并将这些信息发送给木马的操控者，使用户的重要信息泄露。木马程序一般不直接对计算机造成软、硬件的破坏，而且在达成自身目的之后，很多会自动销毁，以免被计算机用户发现后进行追查。

—— 第二十章 ——

英雄还是强盗：黑客的自由抗争

我要颠覆这个黑白颠倒的世界！

——金·达康

与詹姆斯的穷困潦倒相反，同样崇尚自由的人可以换一种方法活得很滋润。比如“盗版之王”金·达康。

平常认识中的盗版者，无外乎一台电脑，几部光盘刻录机，或者更大点的规模，有一条或几条光盘生产线，然后就是街边兜售的小贩。他们会悄悄凑过来：“五元，要不？”金·达康不需要这样小心翼翼，他只需要每天坐在电脑前看看自己的银行账户就行了。

❶ 典型差生的骄傲

金·达康有着纯正的德国血统，同时也继承着德国人特有的聪明、认真、固执等个性，这些个性特点无疑是一名出色的黑客所应具备的。

学生时代的金·达康绝对是个问题少年，他打架斗殴、往女同学的课桌上抹胶水，以及给老师的讲台上放一条拨了毒牙的蝮蛇都收到过“良好

的效果”。

家庭暴力是第一个推手，金·达康的父亲是个酒鬼，每晚除了喝酒就是用腰带狠命地抽打母亲，并把金·达康用绳子绑在阳台上暴晒。学校多次给他找到心理医生，只是心理医生也拿他没办法，他反倒偷了医生的钱包请朋友们吃冰淇淋。直到被学校开除他仍然顶着个坏孩子的名声。

事实上也没有人说他是好孩子。当他的书包再没有用武之地时，他开始琢磨怎么能消磨大把的时间，若是能再挣些钱就更好了。

当时流行的软盘游戏大多很简单，但却绝对的吸引人。金·达康从街边的小店里买来软盘，然后借助一个他自己编写的小程序开始成批的复制游戏软盘，再以低廉的价格卖给周围的人。

互联网刚刚兴起的时候，金·达康敏锐地感觉到这是一个大有作为的天地。他第一时间买来了调制解调器，每天周游于网络之中，当他发现BBS上有关如何入侵他人电脑的帖子时，从小争强好胜的金·达康似乎找到了真正能点燃自己的那支火炬。

从1990年开始，在连续三年的时间里，金·达康破解了多家德国长途电话运营商的长途电话卡账号和密码，并开始在网络上兜售他的战利品。直到被当局逮捕，被拘禁了四个月后才重获自由。

一个19岁的孩子，居然能在防备森严的网络中出入自由，这实在让人吃惊。时至今日，金·达康仍不无骄傲地回忆说，在监狱里的那几个月里，他甚至过得比在家里还舒服，连美国最大的电信巨头AT&T的技术总监都亲自去牢里看望，并渴望他能指点一二，以帮助他们完善自己那漏洞百出的网络体系。

于是，四个月的牢狱并未对金·达康造成任何的心理障碍，相反更刺激了他的野心和骄傲。同时，这些对于黑客防范意识淡薄的公司的不堪一击让金·达康深切地意识到数据安全的重要性。

❷ 云存储与资源共享理念

摆脱了牢狱之灾的金·达康一边继续他风云激荡的黑客生涯，一边对数据安全领域进行全方位的探索，并从一个入侵者的角度展开逆向思维，试图打造一个固若金汤的电子数据的诺亚方舟。

在打开了美国花旗银行、国家航天局和五角大楼的网络之门后，“再没什么高难度的网关能激发我的创造性了。于是我开始转身，全身心地打造一个计算机安全中心。”他与同伴合力创办了美国第一家数据安全公司，主要负责各大机密系统的计算机漏洞的查找和修补，时不时把自己攻破国家航天局的片断拿出来敲山震虎。这一招果然有效，他的公司生意兴隆，甚至国家安全局都要找上门来请他们出马。一时之间金·达康这个名字成了“数据安全”的代名词，一些银行甚至打出了“本系统由金·达康公司负责维护”的广告语。这个名字频频出现在各大媒体的头版头条上，吸引力十足。

“这感觉棒极了。当他们告诉我，我比世界上任何一个玩计算机的人都更聪明的时候，我感觉自己是个超人。”

有着不幸童年的金·达康的确是个喜欢高调炫耀、我行我素的人，他身材魁梧，接近2米的身高和超过130公斤的体重让他看上去更像一个黑社会老大，被称为“世界上块头最大的高科技企业家”。功成名就之后，他在新西兰郊外建造了超豪华的农场和庄园，拥有一架直升飞机和二十多辆顶级豪车。

这个天才的吸金黑客随后把整理了多年的数据安全问题摆上了议事日程。他设想建立一个公共的资源收集站，由用户自由上传数据，并设置数据是否可以共享，这样，在保证隐私资源不至于在本地计算机上因为计算机硬件故障而损失之外，那些共享性的资源还可以为其他需要的人提供尽可能多的帮助。

2005年，金·达康创办了第一个在线资源共享网站“MEGAUPLOAD”。运营的第一年就超过了2亿注册用户，其独特的经营思路让他赚钱赚到手软。

“MEGAUPLOAD”为互联网用户免费提供资源存储和共享服务，资源分为两种，一种是仅供上传人个人使用，只是租用了“MEGAUPLOAD”的空间做存储而已，避免了重要资料的丢失；另一种则是上传后可供其他用户下载使用的，包括各种软件、论文和视频文件。用户也分两种，交费用户可以通过上传资料及被下载频率赚钱，而免费用户除了可以使用的空间小，上传下载的速度受到一定限制外，还拥有一些有限的权限。“毕竟，您需要的是安全可靠的数据备份空间，而我在让这个空间更好用更安全的前提下，要赚钱吃饭。”

在金·达康这块“数据安全”的金字招牌下，“MEGAUPLOAD”如日中天，其股价连续上涨，注册用户也几何级的增长。金·达康不得不在世界各地的网络服务器供应商那里不断地购买中继主机以容纳每天多达几亿个文件的上传量，而金·达康也以一个职业黑客的技术支持向用户保证并做到了数据的万无一失，甚至美国联邦调查局都租用“MEGAUPLOAD”的空间作为刑事案件资料的备份空间。

安全是足够了，作为职业黑客，金·达康知道黑客入侵的方式和方法，并有能力在这方面做到坚不可摧，只是，每天铺天盖地的数据里，也大量繁衍着病毒和盗版软件，而作为数据的存储空间提供商，“MEGAUPLOAD”无论从职业角度还是法律层面上都对这些无权干涉。

国家安全局在提取了某一时段的上传数据分析后得出，平均每分钟至少有数百个未经认证和许可的非法软件被上传和下载，而“MEGAUPLOAD”也因此成了盗版软件的流通和传播基地。

鉴于此，2012年新年美国司法部向金·达康提起指控，称“MEGAUPLOAD”给版权持有者们带来的损失超过5亿美元，并强行关

闭了该网站在世界各地的存储空间。

金·达康没有请律师，他只有一句申辩词。“追求自由的人是无罪的。”金·达康认为“MEGAUPLOAD”只不过提供了资源的共享方案和空间，如果没有“MEGAUPLOAD”，盗版软件还是会继续流通，只不过不是以网络的数字形式，还会依旧停留在光盘的载体之上。

在失去自由的几个月时间里，金·达康仍在构思新的资源共享方式，以一个职业黑客的自由精神诠释信息的公有性这一伟大的事业。在他的构思中，运用P2P技术可以不依赖于服务器而让资源在连入互联网的每一台计算机中流动着共享。他的下一个目标是建立一个在线音乐服务体系，其核心就是P2P技术。

金·达康仅有的一句申辩词胜过了千言万语，法庭认定对其的盗版指控并不成立，这个大块头的高富帅在数月之后又重新回到他位于新西兰的庄园里过着花天酒地的日子了。

“盗版是违法的，但云存储这个理念没有错。”数据存储从最早的软盘、硬盘到光盘，再到U盘，存储介质在变，存储的根本却没有变，那就是，介质的损坏会让数据失不再来，而金·达康开创的云存储相当于在互联网上开通了U盘功能，而且这个U盘空间无限大，且不必随身携带。

非法文件的共享，其行为是错误的，即便不是盗版商，也给盗版提供了极大的方便。但是盗版之王金·达康和他的云存储技术，却因此而改变了常态的存储，使之成为业界通用的新一代存储方式，仅中国国内，就有360云盘、金山快盘等多家云存储提供商。

“假装正义的人说我是强盗，而其他人，则把我打扮成一个英雄。”金·达康，这个80后的杰出黑客，还在为他所信奉的“自由第一”的信念，努力奋斗着。

❸ 软件为什么要收费

哦，我们说到了自由。是啊，自由，人终其一生挣扎着，不过是为了自由这两个字，而这两个字，也正是黑客精神的实质内核。

商品是有形的，有形的商品有其固有的价值，当无形的商品出现以后，如何衡量其价值便成了难题。

计算机是硬件和软件的结合体，失去任何一方都无法正常工作。最早的计算机软件是由计算机硬件制造商负责编写，并固化在硬件之中，连同硬件一同出售。微软公司的起家就在于恰好抓住了计算机硬件迅猛发展过程中软件相对滞后的矛盾。当年比尔·盖茨给IBM编写DOS程序之后，突发奇想，打造了图形界面的Windows系统，使得操作计算机不必死记硬背一长串的命令，只需要鼠标指指点点便可以化腐朽为神奇。Windows的成功使得软件开始从硬件中剥离出来，形成了自身特有的生存和发展之道，并在发展的过程中明码标价。

1976年，21岁的比尔·盖茨在为“MITS Altair”计算机编写软件，只不过有些人把这些软件从硬件中分离出来，当成商品出售给一些小型的计算机生产商。鉴于此，他发表了“致计算机爱好者的公开信”。

“非法的复制应该立法严惩。常识上，硬件是一定要付钱的，而软件却成了可以共享的东西。有谁会在意编写软件的人是不是得到了应有的报酬呢？这种盗版行为的后果只会阻碍那些致力于丰富软件行业的程序员们去编写更好的软件。有谁肯去做一无所获的技术工作？又有哪一位计算机爱好者愿意投入三年的工作量用于编程、纠错、撰写产品文档，最后却免费发布其产品？”

比尔·盖茨是第一个呼吁给软件版权立法的人，事实上他也这么做了。微软公司只靠几行代码就打造了多位排名靠前的世界级富翁。

但并不是所有的人都这么想。一个程序员的快速进步，离不开彼此间

的相互切磋和沟通，而沟通的最有效途径就是代码级的资源共享，而软件立法，设立加密的代码机制，是一种阻碍自由进步、禁锢思想、打击创造力的犯罪，“软件为什么要收费？”理查德·斯托曼的反问很有力度。

❹ 理查德·斯托曼：国家安全局的职业黑客导师

说起来理查德·斯托曼，他和比尔·盖茨还同为哈佛校友。他长比尔两岁，1974年比尔从哈佛大学退学的时候，正是斯托曼握着哈佛的毕业证信心满满地离开学校的时候。哇，那时候，天好蓝，世界好大，整个世界仿佛都装在斯托曼的后花园里。

毕业后的斯托曼在麻省理工大学的人工智能实验室里做程序员，每天周而复始地重复着几乎毫无趣味可言的工作，斯托曼主要负责程序调试和改进界面。在这期间，他最杰出的贡献是为他的黑客朋友们量身打造了一个超级编辑器Emacs。也许很多人并不熟悉这个软件，但业内人士都对这个超强的编辑器耳熟能详。

Emacs[①]基本功能与微软的Office办公套装软件类似，主要用于文字处理和表格数据处理，但是与Office不同的是，Emacs体积小巧，对文字处理来说游刃有余，而且它针对程序员编辑宏代码和程序段有着极大的帮助，可以自动纠错，并给出改进意见，同时在一个软件里整合了大部分的系统操作功能，可以大幅度提高编程速度。更重要的，这个软件的源代码是公开的，任意给这个软件增加或是改进功能都是可以的，体现了技术上最大程度的开放。很多后来搞文字处理软件的程序员都承认，自己在Emacs的源代码中学到了很多技巧，并尊称斯托曼为老师。

在这个层面上来说，斯托曼并不是一个真正意义上搞入侵行为的黑

① 即Editor MACroS的缩写，意为宏代码编辑器。

客，而是给黑客一把攻无不克的利刃。而“黑客”这个词在诞生之初，不是用来形容那些不请自来的入侵者，而是“热爱探索问题，解决问题的一批人”，“热爱编出精妙程序的人”，正因如此，斯托曼一直被业界称作“国家安全局的职业黑客导师”。

当比尔拿着他的“致计算机爱好者的公开信”四处宣扬为软件立法的时候，斯托曼却不以为然。“这违背了程序员的初衷，把自由精神与金钱掺在一起，就像给牛奶里加了醋。”

作为一个忠诚于IT事业的程序员，斯托曼始终认为程序应该是代码公开的，每个人都有知情权，让所有的人自由拷贝和使用才是程序员的终极目的。“至少每个使用Windows的用户在安装系统的时候都会起疑：微软到底往我的机器里塞了些什么？”你花了钱，却没有人回答你，这是不平等的价值交换。

❺ “革奴计划”

斯托曼后来离开了麻省理工的实验室，一个人躲在乡下，一边不断丰富Emacs，一边开始构思他理想中的自由软件运动，而这场运动的核心就是，给用户提供可定制的、公开源代码的软件，软件本身对任何人都不再有任何形式的秘密，任何人都可以打开软件的内核，检查源代码中的错误或漏洞，并自己进行修补，同时去除软件中自己用不到的功能以提高系统运行效率。最关键的，也是自由软件运动的核心内容是：软件是无偿的，免费的，公有的和透明的。

他申请了网站，并注册了“自由软件基金会”（Free Software Foundation），然后独立地编写了几个软件发到网站上，免费供用户使用，并且遵照他的自由软件精神，公开全部的程序代码。他没有收入，住在租来的办公室里。“没有什么能阻止我，我已经决定这么干了。”

渐渐地，他编写的软件开始受到大众欢迎，因其小巧简洁方便实用，同时无论从软件的界面还是功能上用户都可以按照自己的意愿进行二次修改，使之更符合个人的使用习惯。这的确是个好卖点。最关键的是，这一切不仅全部免费，而且“可以教会很多人如何编写程序。这简直太棒了”。

在“自由软件基金会”成立第二年，也就是1985年，斯托曼和大约十个志同道合的人组成团队，合力推出了几个重量级的自由软件，并发布了“自由软件通用许可证”（GPL）和GNU计划，在“总纲”中，斯托曼有如下的发言：“大多数软件的许可证，设计用来剥夺你分发和修改它们的自由。GPL许可证与此恰恰相反，它就是为了保护你分发和修改自由软件的权利，确保这些软件对所有用户都是自由的。”

除了自由，这里没有任何限制。用户彼此复制和使用软件不再被冠以“盗版”，而是体现了人类精神领域中最大渴望的具体实现，那就是，自由。

GNU计划的全中文名称为“革奴计划”，旨在建立一整套科学的计算机软件使用规范，并在此基础上创建一套完全自由的操作系统，“而这套系统不是哪个公司研制出来捆绑销售的，而是你，我，他，我们这些使用计算机的人共同努力完成的一项伟大事业。为保证自由软件的核心思想不被歪曲，我们将建立一个新的软件体制，那就是反版权（Copyleft），任何使用自由软件的人都不必交纳一分钱的费用而得到全部的功能，并且可以自由地使用、复制、修改和发布你的改进成果，借此重现当年软件界合作互助的团结精神。”

自由软件的活力开始越来越多的感染了更多的人，很多电脑精英也加入其中。他们中很多人最初加入这个组织的原因是想多得到一些编程技术，毕竟，自由软件没有经济收入。而当他们进入其中之后才发现，人类伟大的无私精神同样会好人好报。很多著名的企业都伸出援手来资助这个无限自由的组织。而自由软件的制作者大多有着不受约束的创造力，他们

废寝忘食，在很短的时间内开发出众多的自由软件，从最初的基础实用型软件到大型的OA系统，再到计算机底层操作系统，都大有建树。

说到操作系统，除了苹果公司的OS之外，只有微软的Windows了，而在斯托曼的自由软件基金会的带领下，一个全新内核的自由开放的操作系统诞生了，这就是大名鼎鼎的Linux。

Linux是一套免费使用和自由传播的类Unix操作系统，它借鉴了Windows的多窗口多任务图形界面的特点，更注重使用的高效性和灵活性，这套软件包里不仅包括底层操作系统，而且还包括了文本编辑器、编程语言编译器等应用软件，并且最难能可贵的，它兼容了Windows系统生成的各式文件。也就是说，在Windows系统下生成的各种文件，在Linux上基本上都能正常存取，包括目前世界上使用最为广泛的微软Office格式文件。

这完全得益于斯托曼的GNU操作系统。这个操作系统在斯托曼手中只是一个雏形，还在不断丰富和改进阶段，而自由软件基金会的成员们已经对小打小闹的搞些必须借助于Windows系统才能运动的自由软件很不满意了。于是，斯托曼想起了那个被他束之高阁的GNU。

在GNU的基础上，有100余名程序员参与了Linux内核代码编写和修改工作，这些代码按模块式分工合作，每天遍布世界各地的成员们都按照事先约定的模块去完成自己相应的任务，然后投放到自由软件基金会的公用空间，由斯托曼等5人组成的核心组对代码进行规范和整理后上传，交给下一级用户们进行测试。历时数年，1994年3月，Linux1.0终于面世，代码量17万行，按照完全自由免费的协议无偿发布。通过Linux，斯托曼与他的自由软件基金会终于找到了一种属于他们自己的方式把操作系统、计算机硬件和应用软件完美的联合成一个整体。而这一切，都是免费的。

斯托曼曾质问过微软总裁比尔：“你用什么保证你的这套昂贵的Windows中没有后门和监视程序用来监控用户的操作？”但是他没有得到回答，也不需要得到回答。

❻ 软件等于自由

微软有多厉害？看一看计算机的软件业发展过程就够了。

当年微软的第一件成功的作品是DOS操作系统，一个字符界面的计算机底层运动环境，所有的应用软件都运行在DOS下。在文字处理方面，微软显然忽略了中国人的使用习惯，并未在DOS下推动符合中国人使用的文字处理软件，这成全了国内的UCDOS和WPS，在使用汉字的国家里，这两套DOS下的中文操作系统几乎是每台计算机的必备软件。随后微软推出了图形界面的多任务操作系统Windows，在这里，金山公司及时跟进，率先推出了在Windows下运行的新版WPS，而北京希望公司的拳头产品UCDOS当年一套字库就可以卖到上千元人民币，在Windows下却偃旗息鼓消失不见了，在Windows下，金山公司一直以百元左右的价格出售WPS办公软件，而当微软重磅推出Office办公套件之后，WPS毫无还手之力，最后不得不免费向公众开放WPS的使用权（不提供源代码），而且其操作界面和文件兼容性又必须向微软的Office看齐，甚至喊出“中国人用自己的办公软件”，试图用爱国之心留住国人使用WPS的仅剩的热情和兴趣。

微软的霸主地位就是如此凶悍。大有顺我者昌逆我者亡的架势，而且微软的软件都拥有高昂的价格，因为在地球上，只此一家，别无分号。

斯托曼偏偏就斜刺里杀出一刀，这让微软等软件巨头极其震怒却又无可奈何。世界上现有的三大计算机操作系统中，苹果系统只应用于苹果公司生产的计算机上，微软的市场份额占到70%左右，其余的就全被Linux系统拿走了，要知道，当年，Windows系统占领了几乎百分之百的市场份额。

在比尔的眼里，斯托曼是个无恶不作，吃力不讨好的恶棍，而在另外一些人眼里，他是个商业软件领域的野蛮颠覆者，又是无数程序员心中的

“普罗米修斯”，在以“开放、共享、民主、自由”为口号的黑客精神的领引下，斯托曼和他的自由软件基金会非但没有消亡，反而渐次壮大，成为计算机领域最伟大的神。

【黑客知识】

P2P技术：点对点技术（Peer-to-Peer），一种没有服务器主机的资源共享和获取方式，它依赖网络中参与其中的计算机数量和带宽，而不是把依赖都聚集在较少的几台服务器上。与较早的服务器运营模式相比较，P2P技术可以最大限度地利用网络资源，且不使用主服务器，当一个用户开始下载某一文件时，这个用户本身就自动成为服务器，其已下载的部分可以被其他用户搜索并下载，这样，同一时间内下载的用户越多，理论上下载的速度越快，从而可以摆脱服务器模式下同时下载量过大造成的主服务器假死和崩溃。

其缺点是在下载时，几乎霸占着全部带宽，对网络稳定性要求较高，后续的P2P技术已经可以人工设定下载速度以降低对系统的要求。

云存储：作为数据备份的存储设备大致可以分为硬盘、光盘、U盘等几种（软盘由于技术落后稳定性差，现在已基本被淘汰），若是这些存储设备出现故障，保存在其中的数据将不可避免地遭到损坏。一般人的做法是在本地硬盘上保存一份，然后再刻录到光盘或保存到U盘上再做一个备份，但如此的做法操作上麻烦，也很难保证数据的修改同步性。

互联网普及的今天，几乎每一台电脑都可以随时连入Internet，在这个前提之下，云存储作为新一代的存储机制开始出现。狭义的云存储，其工作原理是这样的：在用户的本地硬盘上设立一个专用的文件夹，每个保存到这个文件夹中的文件都会自动被上传到网络上的云存储设备中，而用户每一次登录，系统都会自动查找云存储设备与本地文件夹的内容不同，并按照文件的最后修改时间自动更

新，使得用户无论在哪里，只要接入互联网，就可以使用云存储设备来操作自己保存在云存储设备中的文件，就像在自己的办公桌上操作自己的电脑一样。

广义的云存储概念要比简单的文件自动同步更新要复杂和庞大得多。但其总体理念是共通的，那就是：重要文件的自动更新自动备份同步，而用户不需要随身携带任何存储设备。

—— 第二十一章 ——
黑客就在你我的身边

每一个计算机界的高精尖人士，如果他的电脑生涯不是从黑客开始，或者一辈子没黑过别人的机器，有关他的传奇注定苍白，江湖上也注定不会有他的传说。

——“90后”黑客“食指上的爱”

❶ 李开复的黑客玩笑

李开复20年前是美国哥伦比亚大学法学院一名学生，与美国现任总统奥巴马是同班同学。1998年，李开复加盟微软公司，随后创立了微软中国研究院，2005年7月起任谷歌全球副总裁兼中国区总裁一职。2009年9月离职，随后创办了创新工场。

就读哥伦比亚大学时，由于法学专业实在枯燥，性格开朗活泼的李开复申请转到了计算机系，原因是“我编程比谁都快，读法学睡着的比谁都快”。

李开复在学校时，就把手中的计算机变成了自娱自乐的工具并深深地陶醉其中。有一次，他“黑”了一个同学的论坛账号，然后用对方的账号发帖，声称自己是选美小姐，希望交到一个帅气的男朋友。随后，账号的

主人收到一大堆让人摸不着头脑的邮件。

还有一次，一个同学让他帮忙写一份重要的编程作业，李开复借口有事推掉。同学无奈之下自己开电脑进行编写，作业快写好时，点击保存，弹出错误提示，称作业已丢失。重写，写好后保存，又出来提示错误，称再次丢失。同学郁闷万分，自认倒霉，在关机时弹出新的提示："刚才是个恶作剧，作业已帮你写好。李开复。"

如果李开复自己不承认，恐怕没有人会想象到一个全球化信息产业的总裁也会可爱到如此地步，其实那些不苟言笑的人们，也都有其可爱至极的一面。

❷ 海信被黑

互联网日新月异地改变着人们的工作和生活，而黑客的存在可以说是互联网的最大威胁。有数据表明，平均每15秒就会有一起黑客事件发生，全球范围内每年因黑客造成的经济损失就超过500亿美元。如此众多的经济损失直接原因就在于计算机的使用者忽视网络安全，一项调查发现90%以上的个人和单位用计算机存在严重安全漏洞，甚至一些政府机构和银行等也不能幸免。

如此众多的安全隐患给黑客留下了最广大的施展空间，解决的办法除了及时更新系统漏洞外，就是安装网络防火墙。

系统自带的防火墙已经不能满足用户的需要。于是，各大计算机安全公司瞄准这一市场，纷纷推出自己的更高级别的防火墙系统，仅国内就有天网、江民、瑞星等多家公司把防火墙系统作为主打产品推向市场，加之国外产品的渗透，使得防火墙市场竞争自20世纪90年代初期开始就进入到白热化状态。

海信公司一直致力于家电产品的研发，在国内具有较高的知名度，打

出品牌效应之后，海信开始进入计算机市场，成功地推出了自主品牌的电脑产品，在此基础上，2000年夏天，海信公司终于决定进军市场潜力巨大的计算机防火墙领域。

在现有的防火墙系统技术催化下，海信花大力气研发了名为“8341”网络防火墙产品，它“弥补了前代防火墙的种种缺陷和隐患，从而更加安全可靠。‘8341’是世界是最伟大、最安全的‘警卫部门’”。海信在集团内部进行了多次模拟攻击性实验，结果令人满意，随后其产品经过了公安部门的检测并获取了生产许可证。为了更快地打开防火墙市场，海信公司突发奇想，以50万元的巨资邀请国内外黑客进行攻击测试。“在信息社会，信息产品虽然需求量剧增，但海信公司没有盲从，而是冷静地等待技术和市场的成熟，这一次，海信将以完美的防火墙产品进入市场，作为海信‘触网’的最佳契机。相信这一次的攻击展示不会令海内外一直关注海信产品的同仁及用户失望。”海信公司特意在北京电信申请了接受黑客攻击的IP地址（210.12.114.58），并在北京最大的电子产品市场中关村立起了巨大的LED显示屏，24小时不间断地显示主机工作状态及接受到的攻击信息、即时公布攻击的来源、方法、数量及防火墙的工作状况。

根据海信制定的游戏规则，2000年8月21日至9月1日的十天时间，一旦有黑客获得了防火墙后面服务器的指定文件（fw3010ag.test），或者修改了服务器的页面，就视为成功攻破防火墙，海信将给予50万元的高额奖金作为检测费。

能够正当攻击一个知名品牌，还有高额的奖金，这无疑具有巨大的吸引力。50万元谁能拿走？海信防火墙中关村“设擂”挑战全球黑客，到底是魔高一尺，还是道高一丈，到底是黑客的矛利，还是海信的盾坚？挑战从一开始就扣人心弦。

LED显示屏上，攻击防火墙的地址来自五大洲十几个国家，甚至还收到美国国防部网络中心、弗吉尼亚陆军特种战术和技术中心的“垂青”；国内的攻击更是遍及各地，仅仅四天时间，攻击计数器显示的数字已接

近六万次，攻击手段也几乎包含了当时已被发现的全部主流攻击方式，ICMP攻击、碎片攻击、WEB服务器攻击、UDP攻击、远程溢出攻击、FTP服务攻击、后门攻击等不一而足，在规则允许之外，还时不时夹杂了众多的恶意攻击，堵塞通信端口、反监测渗入等手段也逐一登场现身，海信的防火墙果然不负重望，接受了近一百个小时的攻击后仍然固若金汤。

8月25日，接受攻击测试的第五天，显示屏依然是防火墙的胜利消息，而一个坏消息却在显示屏以外成了一盆兜头浇下的冷水：一个署名为“黑妹”的黑客篡改了在海信公司首页（http://www.hisense.com.cn/）并在首页上放了一封措辞严厉而又幽默搞笑的信。

“尊敬的海信副总裁王培松先生：

21日您悬赏50万人民币向公众公开授权对贵公司生产的防火墙进行攻击测试，司马昭之心路人皆知，无非为了炒作。如果贵公司对自己产品有绝对的自信并愿意接受公正、公开的攻击测试倒也无可厚非，但贵公司却把一堆废钢烂铁摆上网，公布一个Ping不通的地址，这简直是自作聪明的懦夫行为，是对黑客的极大侮辱，对公众的绝对欺骗。我们相信，如果贵公司在网络安全领域真的有独到之处，应以身作则，利用自己的产品，保障自身网络安全，否则何以保证客户利益？有何颜面立足网络安全领域……”

众皆哗然，人们拭目以待。随后海信公司发布声明，声称黑客违反了游戏规则：

“‘黑妹’声称的IP地址无法Ping通是由于测试以来，众多的黑客向防火墙所在的IP地址不间断地发送垃圾数据包，占用了这台服务器的接入带宽资源，使得其他的攻击难以进行甚至无法进行。从8月22日上午开始，有大量的数据包以每秒4000~6000个的速度涌向海信申请的IP地址，这种恶性攻击用无用数据占用了海信90%以上的网络带宽，导致能够对海信申请的IP地址进行测试攻击的网络爱好者非常少。黑客的恶意程序每隔几十秒就会停止攻击，检测防火墙是否工作，然后再进行攻击。这种攻击

不可能是哪一个人能够做到的，应该是企业集体行为，海信竞争对手的嫌疑最大。”

黑客在所谓的IP地址无法Ping通之后，没有继续跟防火墙正面交锋，转身黑掉了防护薄弱的公司主页，而海信公司的网站并没有安装这种防火墙。

以上的解释显然无法让人们感到满意。既然没有不允许恶意攻击的限定，那么采取何种手段对付防火墙都将是被允许的，这样一个号称无懈可击的防火墙产品，开发者居然不首先在自己的网站上使用，却要拿出来接受公众的挑战，其动机难免不为人们所怀疑。

防火墙产品不是万能的，再坚韧的防火墙，被越过之后便形同虚设。虽然严格意义上来讲，海信的防火墙还是没有被攻破，但在大众心目中，防火墙的形象却大打折扣。

❸ 第一个黑客与他的哨子

黑客是一群人，是一个群体的代名词，自从世界上出现了计算机这东西，黑客便如影随形悄然现身，没有谁敢声称自己是世界第一，也没有人敢说自己资格最老，但世界公认的第一个被称作黑客的人，他所使用的工具不是电脑，而是一只哨子，这不能不说是个传奇。

出生于1944年的约翰·德雷珀（John Draper）从小就跟随自己做空军工程师的父亲周游世界，生性随和的他也自然在全球各地结交了不少朋友，每次回到家，他自己就整天坐在椅子里给他遍布全球的朋友们拨电话，父亲每个月都会对着那些高额的电话费单据暴跳如雷，最后迫不得已叫停了家里的座机，把约翰·德雷珀逼到了街角的电话亭里。1964年他子承父业，参加了空军。驻防阿拉斯加时，他仍然恶习不改，整天琢磨怎么混进长官办公室去煲电话粥，两年后不务正业的约翰·德雷珀被军队开

除，原因之一是他居然无意之中把电话打到了总统尼克松的办公室。

退伍之后的约翰·德雷珀结了婚，有了属于自己的家，第一件事不是和新娘子喝交杯酒而是申请安装了一台电话。接下来的更多时间里他把新婚妻子扔到一边，继续他的电话梦。

一个下午，邻居来找他打球，他目不斜视仍旧全神贯注地忙于接打电话，邻居恶作剧地把挂在脖子上的哨子突然吹响了一下，约翰·德雷珀虽然不为所动，却惊奇地发现，哨声之后，他的电话还保持着畅通，电话上显示通话时长的数字却突然停止了。

这个发现让他兴奋不已，他立即买回了大大小小的哨子做实验，原来哨子产生低频声波恰好可以用来欺骗电话交换机，系统收到这个频率的信号以为通话中断便停止计费。从此他便用这个不算高精尖，但绝对另类的法子夜以继日地拨打免费国际长途却不用付一毛钱，每次拨通电话一两秒钟他就抓过哨子拼命地吹上一下，然后美美地享受自己的好时光。

如若不是那个多事的话费追缴员，他的好日子不知道要持续多长时间。1972年，一位电话缴费员奇怪地发现约翰·德雷珀的电话账单很有趣：每个国际长途电话的通话时长都只有短短一两秒钟。后来他可以算得上是因为“一只哨子”的原因而被判入狱两个月。

就是这个吹哨子打免费电话的家伙，被戏称为“世界上第一个黑客”。受他的启发和影响，在计算机成为普罗大众都能使用的社交工具之后，那些黑客们也大多是从设法打免费电话开始自己黑客生涯的，只不过他们需要用电脑连接周边的电信局，想办法去取得最高级别的管理权，而不是在脖子挂一只其貌不扬的哨子就解决问题。

❹ 都是天才惹的祸

2007年6月，美国宾夕法尼亚大学工程学院的网络服务器在历经十余

个小时的抵抗之后终于一病不起，就在这十几个小时里，服务器接受到超过7万次下载请求，从而造成系统崩溃，而平时的日下载请求量一般不超过500个。

黑客攻击的手段中比较常见的就是以不断申请下载链接的方式借机在系统中寻找到可以入侵的漏洞，在黑客登录服务器的蛛丝马迹中，FBI的探员发现两个IP地址非常可疑，系统日志表明，仅从这两个IP地址发出的下载请求就高达6.8万多次。

历经半年时间，经过FBI探员抽丝剥茧般地细心搜寻，终于找到其中一个IP地址的所有者，新西兰一个绰号“头号杀手”的电脑黑客浮出水面。2007年11月30日，警方突袭“头号杀手”位于新西兰汉密尔顿的家，将这家的小主人欧文·托尔·沃克带离住宅。在FBI总部，不满17岁的沃克很快交代了整个事件的经过，通过沃克的供述，FBI顺藤摸瓜，成功地破获一个涉案人员极多，涉案金额重大的通过互联网实施经济犯罪的代号“A组”的跨国犯罪团伙。

这个团伙通过招募电脑黑客，以高利润为诱惑请他们编写“僵尸程序”非法侵入并成功地控制全球约130万台个人主机，窃取机主的网络账户信息和银行密码，从而偷盗资金、操控股票交易，短短一年的时间里就造成了2600万新西兰元（约合2000万美元）的损失。其中，沃克非法获利3万多美元，一审被判处十年监禁。

以沃克为代表的黑客集团运用先进的计算机算法和极其巧妙的编程思路，编写了十分复杂而隐蔽的黑客程序，并约定遍布全球的集团成员步调一致，在同一时间登录同一网站，造成网站瞬时在线人数剧增，从而迫使网站服务器因不堪重负而丧失抵抗能力，其编程技术的“科技含量”高得惊人，连从事电子技术犯罪侦测工作多年的专家也不得不心悦诚服地说，沃克编制的黑客程序是迄今为止他们遇到的最先进的一种，而直至被捕，这个事件的主人公沃克仍不满17周岁。

随后新西兰媒体的报道则更加惊人，法庭可能对沃克轻判，轻判的原

因不仅仅是因为沃克的年龄，更多的是在例行的体检中，医生发现沃克患有一种十分罕见的疾病——埃斯博格综合症。

与帕金森综合症一样，这种病症的命名源于发现者的名字，这种发病率仅有数1/100000的疾病具有高度遗传性，青少年时期症状极其明显，发病者不爱说话、不善社交，甚至可能会有语言障碍并表现出肢体的不协调性，常被误认为是性格内向而被忽略，部分发病者表现为具有极高的智商并在数学逻辑等方面具有超强能力，常会心无旁骛地迷恋某一兴趣点，对一些逻辑思维要求较高的领域更为专注，比如音乐、绘画、数学和计算机，并能够在这些方面取得超人成就。很多历史名人都患有埃斯博格综合症，如画家梵高、音乐大师莫扎特和著名的唯心主义哲学大师康德等。

沃克从小就少言寡语，不合群的他常一个人躲在角落里摆弄积木，整天一声不响。在学校里他常常被人欺负，九年级时不得不退学。退学之后他便一头扎进计算机世界里不能自拔，每天与键盘鼠标为伍并乐此不疲，父母一度欣慰地认为他总算找到一种与这个世界的沟通方式，却没想到他将为此付出坐牢的代价。

天才才能得天才的病，也只有天才才会做天才的事。因为天才，所以17岁的沃克成为了一名技术高超的黑客；也因为天才，他造成了重大的经济损失而被判刑；更因为天才，沃克又可以获得减刑。

都是天才惹的祸。

❺ 盖茨的第一个职业居然是黑客

用过计算机的人都不会对比尔·盖茨的名字感到陌生，成为比尔·盖茨式的人物几乎是所有人的梦想。但是很少有人知道，比尔·盖茨第一次创业始于16岁，并且和大多数初出茅庐的创业者一样以失败告终，他的第一个职业，居然也是接近于黑客式的。说他“接近于黑客式”的职业，实

际上是说他在合法地使用黑客技术。

当时13岁的比尔·盖茨与长他两岁的艾伦还在中学读书，放学之后，他会和艾伦一起跨上自行车到离学校数英里之外的“计算机中心公司”（Computer Center Corporation）上夜班，没有工资，仅仅是为了可以免费使用计算机。在20世纪60年代末期，即便是向美国这样的发达国家，计算机也仅仅被为数不多的实验室和政府机构拥有。在比尔·盖茨所在的学校里，每周也只能轮流上机一小时，这短短的一小时显然不能满足比尔·盖茨这样对计算机痴迷到发狂的人。于是，当计算机中心公司找到他并要求他给公司承接的软件工程查找错误时，比尔·盖茨欣然应允，虽然没有报酬，但可以无限制地免费使用计算机，仅这一个好处已经让比尔·盖茨感到狂喜了。

当时的比尔·盖茨与艾伦有着与年龄极不相称的计算机技术，甚至很多专业计算机操作人员也望尘莫及，对于计算机中心公司交给他们的任务可以说是手到擒来轻松得很，计算机中心公司的软件程序很复杂，难免存在不少错误，而这些错误在日后的实际应用过程中会影响系统的正常运行，这会对公司造成极大的负面影响，比尔·盖茨每晚在这些程序中反复实验，意在发现软件中最细微的缺陷。几个月后，由比尔·盖茨和艾伦上交的《问题报告书》居然长达300页，内容涉及源代码的“硬伤”及错别字等不下几千种错误，在挑错之余，深谙其中微妙的比尔·盖茨两人甚至擅作主张地修改了不少程序代码“以使程序看上去更稳定、更完美”。在那份报告书中，比尔·盖茨经常会不经意地流露出嘲讽之意，某人的编程思路有问题，某人在某个公式的计算上犯了三次同样的错误，某人用500行代码实现的目的经我的修改只需要160行代码，这让那些专业的计算机工作者很没面子，最终计算机中心公司为了顾全大局，不得不忍痛解雇了比尔·盖茨与艾伦两人，虽然“这两个家伙的工作真的无可挑剔”。

盖茨“失业”之后，为了寻求更多使用计算机的机会，转而瞄上了当时与IBM一起从事巨型计算机生产的“控制数据公司”（CDC），这家公

司建有一个全国计算机网Cybernet，这在当时是很少见的可以只靠计算机就能实现全球通信的网络，CDC声称此网无论何种情况下都是安全可靠的。就是因为这句话，年纪不大的比尔·盖茨决定挑战一下该公司的网络。

凭借着数十台与之相连的周边服务器维持它巨大的数据吞吐，只要能控制其中的一台，就可以利用这台机器控制Cybernet网络系统的主机，沿着这一思路，比尔·盖茨与艾伦两个人成功地溜进系统，并在其中所有的计算机上安放了同样的“特别程序”，并成功地导致了这套“无论何种情况下都是安全可靠的”系统长达十几个小时的运转失常。

与所有的黑客下场一样，比尔·盖茨和艾伦最终没能逃脱惩罚，法庭判决一年之内不准二人接触计算机成品和相关的计算机软件。

可是这两个淘小子怎么可能乖乖听话呢？当英特尔推出8008芯片时，两个人第一时间弄到了一块，并将其应用在自己改造的计算机上，再经过一个多月的努力赶制了一套程序，这套程序基于城市道路交通监视器获得的数据，负责把城市各地传来的消息进行汇总和整理，从而为城市交通系统做最及时的数据分析。看得出比尔·盖茨和艾伦二人对这套系统抱有极乐观的态度，认为它在不久的将来就可以改变交通现状，甚至还平生第一次为一套软件成立了公司，他为自己的新公司取名为交通数据公司（Trof-O-Data），但不久之后这家公司就倒闭了，原因是市政府的各大部门经过慎重考虑，实在无法相信两个年龄加起来仅仅35岁的少年的作品。

第一次经商失败后，艾伦上了大学。一家大公司TRW公司听说艾伦与盖茨在CCubed的成就，主动找上门来为两人提供了一份开发软件的工作，年薪高达3万美金。既能满足计算机欲望，又有钱好赚，巨大的诱惑让艾伦离开了大学，盖茨也从中学请假，两人重新开始编起软件来了。这一干就是几十年，从而成就了世界计算机界的一大传奇。

谈及自己青少年时的经历，盖茨说：“那时已经很难把我同一台能如

此准确无误地展示我的成功的机器分开了，我已经深深陷进去了。”

而这其中，除了严谨的逻辑思维之外，比尔·盖茨也时不时地流露出与他的年龄相符的少年式的可爱，他在为自己所在的学校编写学生座次排序软件时，偷偷地加进一些指令，使自己成为班上唯一一个周围坐满了女生的男孩。

【黑客知识】

Ping指令：Ping（Packet Internet Grope），互联网包探索器。是微软操作系统自带的一个可执行命令。利用这个命令可以检查网络是否连通，可以帮助分析并判定网络故障。对于网络管理员或者黑客来说，这是第一个必须掌握的网络管理命令，其工作原理是利用计算机IP地址的唯一性，给目标IP地址发送一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通，网络传输的速度是多少等相关信息。

防火墙：一个由软件或硬件设备组合而成的在内部网和外部网之间的保护屏障，从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、数据包过滤和应用网关4个部分组成。一般个人用户使用软件防火墙，而一些有保密需求的单位则使用功能更强大的硬件防火墙，硬件防火墙的价格昂贵，非个人用户可以负担。文中提到的海信公司的防火墙则属于软件防火墙。《达·芬奇密码》一书的作者、当今美国最著名的畅销书作家丹·布朗的处女作《数字堡垒》中，美国国家安全局（NSA）斥巨资建造了一台可以破解一切密码的机器——万能解密机。这台超级电脑帮助NSA挫败了无数恐怖分子的阴谋，但这台电脑也能截获普通人的电子邮件，其强大到足以让这个世界没有隐私和秘密可言，面对这样一台机器，人类将何去何从？在本书的最后，NSA首席密码破解专家苏珊·弗莱切亲眼目睹了万能解密机的防火墙系统被攻破。全书情节起伏跌宕，煞是好看。

“CPU”及8088处理器：8088是一个英特尔公司（Intel）以8086中央处理芯片为基础而开发的微型个人计算机中央处理器，在个人计算机研究领域中具有里程碑式的意义，它拥有16位元暂存器和8位元外部资料总线。Intel 8088处理器的成功，将英特尔带入“财富杂志500大企业排行榜”，并被评为“20世纪70年代最成功的企业”之一。Intel 8088晶体管数目约为2.9万颗。在8008的基础上，英特尔公司再接再厉，在随后的几年时间里连续推出了80286、80386及80484中央处理器，也就是我们过去常说的“286、386”系列电脑的中央处理器，后来按照相关法律，纯粹的数字不可以作为产品的名称，英特尔公司遂将中央处理器命名为“Pentium”（奔腾），第一台Pentium处理器于1993年3月推出，在火柴盒大小的芯片上集成了310万个晶体管，由此，个人电脑进入了“奔腾时代”，计算机在之后相当长的一段时间里也习惯地以“奔三、奔四”区分。

CPU是一台计算机的运算核心和控制核心。电脑中所有操作都由CPU负责读取指令，对指令译码并执行。其功能主要是解释计算机指令以及处理计算机软件中的数据。所谓的计算机的可编程性主要是指对CPU的编程。

在计算机出现的最初几十年里，英特尔公司是世界上唯一一家可以研制和生产中央处理器的厂商，目前为止，英特尔公司的中央处理器市场份额占到75%以上，其他还有AMD、IDT以及中国台湾的VIA中央处理器和中国自主知识产权的龙芯中央处理器，最高级的中央处理器目前已经能在四平方厘米面积上集成近3亿个晶体管。

后记

致中国4亿网民

2011年1月，中国互联网络信息中心（CNNIC）在京发布的《第27次中国互联网络发展状况统计报告》称，截至2010年12月底，我国网民总人数达到4.57亿，手机网民达3.03亿，按发展概率计算，2011年中国网民将突破6亿。而据一个民间网络调查数据显示，中国网民中的黑客与曾经尝试过黑客行为或进行过黑客技术研究的人数，占全体网民总数的31%以上，这数字庞大到令人震惊。有据可查的中国最小的黑客来自贵州，一个刚满7岁的小男孩在QQ空间中发现了其幼儿园老师最新的空间日志名为“期中测试题”，于是通过简单的猜测试验破解了老师的QQ密码，并在考试的前一天，把试题包括正确答案以他认为合适的价格卖给了至少六个同学。

美国人造就了黑客这个昂扬着斗志、袒露着个性和锋芒的自由职业，如同他们当年挺进美洲西部，而西部造就了牛仔帽、工装裤，短枪烈马纵横荒漠的牛仔。

当美国国防部将阿帕网（ARPANET）投入到民用计算机领域后，就注定了整个世界将为之改变，从此，继各种交通工具以外，一根细细的网线在更深层次的意义上将整个世界联系在一起。

黑客也随着第一代计算机的成型，逐渐发展壮大，他们以“一切信息都应该是免费的”为终极目标。他们乐观地相信，任何一个人都能在计算

机上创造艺术与美，计算机能够使生活变得更美好。

这些掌握着最精深的电脑知识、热血沸腾的人们在一个虚拟的世界里让自己的个性得到自由地释放，他们迎接挑战并信心十足，以堂·吉诃德的方式实现着现实里无法触及的冒险与征服。他们试图凭一己之力造就一个属于所有人的大同世界。

与病毒的制作者不同，黑客始终具有一种处于正邪之间的丰满鲜活的个性色彩，人们憎恨病毒，却对黑客始终抱有怜悯和赞叹之情，即便是现在的黑客更多的是以经济利益为出发点，而不再以探索计算机技术前沿为己任。康沃尔在《黑客手册》一书所说：“黑客活动的乐趣和报偿纯粹是智力上的”。这句话现在只适合于最初的单纯以技术博弈取乐的黑客精神，而人们更愿意相信，21世纪的黑客，多数已经变为巧取豪夺的无“道”之贼。

可是无论是谁都更愿意将其归为“电脑捣蛋分子”而不是“电脑破坏分子”，无论是谁都不忍一笔抹杀黑客的执着和可爱。

的确，虽然有为数众多的网络诈骗、欺诈、盗号等，但黑客的主流仍显得很健康，很阳光，尤其在中国，甚至被冠以“红客”美誉，这不能不说是个奇迹。

黑客中很多人是想以一种特殊的方式留名青史，在技术崇拜中把自己锻造成榜样和楷模，由此，他们期望自己群体的存在可以在史册的一角以一种文化现象的形式被认可。于是，只要是他们可以涉足的舞台，他们都期望能够登台表演。但他们自我完善，或者说体现自我存在的方式太另类了，这其中也难免有害群之马，使得“入侵的艺术”经常会遗憾地沦为侵犯和杀戮，严谨的思维和并不坚定的立场使他们在黑白之间摇摆不定，那些锋芒毕露的探索精神和强大的攻击力量又使他们成为身怀利器的破坏者，以身试法者亦不在少数。

于是，正义与邪恶的界限在他们心中时而清醒，时而模糊，而做出抉择并不容易，随着理智的成熟和年龄的递增，好奇心的消减和激情的逝

去，以及了解世界的角度和思索事物的焦点的转变，逐渐使他们其中的很多人急流勇退，隐迹封刀告别江湖。这是典型的“黑客式的成熟”。

有数据显示，中国目前的4亿网民中，平均年龄仅有24岁，这是一个庞大的处在青春期的人群，他们好动，易怒，有着年龄带来的叛逆心理，且缺乏成熟的理智的思维判断体系，而黑客所具有的一些特点正与他们这个年龄段人们的心理需求所契合。

但不可否认的是，这也是一个最具生命活力和创造力的群体，他们体力充沛，精神饱满，永远有着强烈的好奇心和果敢的行动力，他们以网络为阵地，在“QQ农场”和“极品飞车”等虚拟游戏的间隙里，也时常以黑客的身份冲锋陷阵，在现实世界中寻找刺激。

黑客行为的最终结局有时往往是两败俱伤，并且难免伤及无辜，一些经常从事黑客活动的人，在攻击他人的同时，其自身被攻击的概率在40%以上，平均每周要重新安装一次操作系统，真是杀敌一万自损八千。因此，即便是出于道义，若是造成他人的损失，黑客本身也要承担责任。

《刑法》第286条：“故意制作、传播计算机木马、病毒等破坏性程序，影响计算机系统正常运行，后果严重的，构成破坏计算机信息系统罪。违反国家规定，入侵国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”

由此可见，无论是从道德角度还是法律意义上来说，任何侵入他人计算机的黑客行为都是违法的，都随时可能遭到法律的制裁，即使是以正义之名。黑客的危险也不仅仅是遭受对方的报复性打击，法律的无情和公正同样要使黑客的行为付出代价。而作为普通网民，使用正版软件、不从事黑客攻击、不跟风而动则是最基本的准则，互联网战争永远没有压倒性胜利，结果只能是两败俱伤。

但互联网是一个各种信息无所不包、引人入胜的虚拟世界，每个人都无法完全摆脱这个世界，互联网对于黑客来说，就是虚拟世界里的一个竞技场，一个比武场，一个秀场。不敢想象，如果互联网上缺少了黑客，这

个虚拟的世界将会怎样的落寞和无趣？

显然，只要计算机技术在进步，黑客们作为游走在技术边界的探索者就不会消失，人们希望做到的无非是在把黑客所能带来的负面影响降低到最低限度的同时，让黑客们保留对于技术探索的执着，使其特立独行的精神贯穿整个信息时代。

致谢

三年了，这本书辗转于多家出版社的案头，每每下到印刷厂之前被截断横流。现在，这本书终于可以见到天日，再来端详这些文字，居然有些不知所措的陌生感。

十年前，辞了工作在乡下隐居，每天夹着笔记本电脑混迹于江边打渔的舟船之间，吸几口江上的风，喝几口乡下酒坊的烧刀子，零零散散地敲出些字来，以供某杂志连载。与此同时，应某校长朋友之托，开始整理有关黑客和计算机的相关资料，然后每周去课堂上误人子弟换些酒钱。再后来，渐渐地，这些断断续续零零散散教案终于有了些书的样子。

再后来，忙于海南的一个剧本，于是这本书便在出版社的案头渐渐生灰。所幸，有湘潭君悦传媒发展有限公司王国军总经理的鼎力相助，没有他的更正和校勘，这本书还不知要压多久；还要感谢作家马淑敏、卢海娟、候拥华、刘清山、刘黎莹、刘学正、马晓伟、陈华清、汝荣兴、周国华、田玉莲、许冬林、张珠容、赵经纬、刘述涛，感谢这些作家认真校正着这本书的每一个字。

一个东北男人，在江南的湿雨里，向翻开这本书的每一位读者问好。正是由于你们的热心，才可以为这本书压一枚用目光雕成的、小小的书签。

刘　创

2014年5月于多雨的钱塘江畔